HP System Management Homepage 7.2 User Guide

HP-UX, Linux, and Windows Operating Systems

HP Part Number: 509679-009
Published: February 2013
Edition: 1

© Copyright 2009, 2013 Hewlett-Packard Development Company, L.P.
Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

AMD and ATI are trademarks of Advanced Micro Devices, Inc.

Adobe and Acrobat are trademarks of Adobe Systems Incorporated.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel and Itanium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Red Hat is a registered trademark of Red Hat, Inc. in the U.S. and other countries.

UNIX is a registered trademark of The Open Group.

Java is a registered trademark of Oracle and/or its affiliates.

Microsoft® Windows® XP and Microsoft® Windows® Server are U.S. registered trademarks of Microsoft Corporation.

Warranty

HP will replace defective delivery media for a period of 90 days from the date of purchase. This warranty applies to all Insight Management products.

Contents

1 Product overview....6
Product features....6
HP SIM....6
2 Getting started....7
Signing in....7
Starting HP SMH from Internet Explorer....8
Starting HP SMH from Mozilla or Firefox....9
Starting HP SMH from HP SIM....10
Configuring firewall settings....10
Windows....10
Linux....11
Red Hat Enterprise Linux 4, 5, and 6....11
SUSE Linux Enterprise Server....12
Configuring timeout settings for HP-UX....13
Configuring SMH Service Timeout....13
Configuring SMH Session Timeout....13
Automatically importing certificates....14
Signing out....15
3 Scenarios....16
IP Binding....16
IP Restricted Login....16
Local Server Certificate....16
Port 2301....16
Kerberos Authentication (Windows only)....16
User Groups....16
Alternative Names (Windows and Linux only)....16
4 Navigating the software....17
Information areas....19
Icon view....21
HP SMH pages....23
5 The Home page....25
Component Status Summary....25
Overall System Health Status....25
6 The Settings page....26
SNMP webagent box....26
SMH Data Source category (Windows and Linux only)....26
SNMP Configuration category (Windows and Linux only)....26
UI Options category (Windows and Linux only)....27
System Management Homepage Box....27
UI Properties category....27
User Preferences category....28
Security....29
Anonymous/Local Access category....30
IP Binding category....31
IP Restricted Login category....32
Local Server Certificate category....34
Port 2301 category....35
Timeouts category....37
Session Timeout....38

UI Timeout....38
Trust Mode category....38
Configuring Trust Mode....39
Trusted Management Servers category....41
Kerberos Authentication category (Windows only)....41
Kerberos Authentication Procedure....41
HP SMH Kerberos Authentication....42
Kerberos Administrator....43
Kerberos Operator....43
Kerberos User....44
User Groups category....44
Administrator Group....46
Operator Group....46
User Group....47
Handling (proper) of the HP SMH certificate revocation....47
Detecting and handling memory leak at runtime (Windows only)....48
Alternative Names Certificates (Windows and Linux only)....48
Menus (HP-UX only)....48
Add Custom Menu (HP-UX only)....49
Remove custom menu (HP-UX only)....49
7 The Tasks page....50
8 The Tools page (HP-UX only)....51
9 The Logs page....52
System Management Homepage Log....52
SAM Log....52
Httpd Error Log....52
Supported languages....53
10 The Installed Webapps page (Windows and Linux only)....55
11 The Support page....56
The Help page....56
Search form....57
Credits....57
12 Command Line Interface configuration....58
Anonymous Access....58
Display Current Settings (Windows and Linux only)....58
Local Access....58
IP Restricted Logins....59
IP Binding....59
Trust Modes....60
Restart service....60
Reject Program Admin Login (Windows and Linux only)....60
Win32DisableAcceptEX....60
Enable/disable SSL v2....61
Log Rotations (Windows and Linux only)....61
Rotate Log Size (Windows and Linux only)....61
Maximum Number of Threads Allowed....61
Maximum Number of Sessions (Windows and Linux only)....61
Session Timeout....61
UI Timeout....62
Log level....62
Port 2301....62
Multihomed certificate alternative names list....62

Custom UI....63
Log-based directory....63
Configurable logging....63
Autostart mode....63
Httpd Error log....63
Icon view....64
Box Order....64
Box Item Order....64
Kerberos Authentication....64
User Groups....65
Help message....65
File-based Command Line Interface....65
Command Line Log Reader....66
SSL Cipher Suite configuration....67
Change locality....67
Detecting and handling memory leak at runtime (Windows only)....67
13 Troubleshooting topics....68
14 Service and support....79
Support and other resources....80
Information to collect before contacting HP....80
How to contact HP....80
Security bulletin and alert policy for non-HP owned software components....80
Subscription service....80
Registering for software technical support and update service....80
How to use your software technical support and update service....81
HP authorized resellers....81
New and changed information in this edition....81
Related Documents....81
Typographic conventions....82
A HP SMH file locations....84
B HP SMH Ciphers....86
Ciphers used in HP SMH....86
15 Documentation feedback....87
Glossary....88
Index....93

1 Product overview

HP System Management Homepage (HP SMH) is a web-based interface that consolidates and simplifies single system management for HP servers running the HP-UX, Linux, and Microsoft Windows operating systems. HP SMH aggregates and displays data from Web Agents and other HP Web-enabled System Management Software that include:

- HP Insight Diagnostics
- Array Configuration Utility
- HP Software Version Control Agents

HP SMH enables you to view detailed hardware configuration and status data, performance metrics, system thresholds, diagnostics, and software version control information using a single interface.

Product features

HP SMH provides the following enhanced security and streamlined operations for HP servers running HP-UX, Linux, and Windows operating systems:

- Browser access using operating system-based Secure Sockets Layer (SSL)-secure authentication.
- Common HTTP and HTTPS service for HP Insight Management Agents and utilities, for reduced complexity and system resource requirements.
- Simplified architecture for implementing HTTP security and HP management updates.
- Access control through Network Interface Card (NIC) binding and advanced configuration features for individual and groups of users.
- Broad operating system and browser support.
- Automated log collection via `smhassist`.

  This feature is available only on HP-UX 11i v2 and HP-UX 11i v3 systems.
- Command Line Interface (CLI) - `smhconfig` - provides users with administrator rights access to set values through the command line.
- Facility to disable port 2301.
- Logging into `syslog` the activities related to login and logout performed on HP SMH.

  This feature is available only on HP-UX 11i v2 and HP-UX 11i v3 systems.
- Consolidated API logging for HP SMH and WebApps: Provides an option to log the critical and major events of both the HP SMH and its WebApps to the system log for viewing and auditing.

HP SIM

HP SMH is tightly integrated with HP Systems Insight Manager (HP SIM). You can easily navigate to HP SMH from the **System Lists** and **System Pages** in HP SIM.

NOTE: Accepting the HP SIM certificate is the default behavior.

2 Getting started

To get started with HP System Management Homepage (HP SMH), use the following information when configuring HP SMH and setting up users and security properly.

To configure HP SMH:

- On Linux operating systems, HP SMH is installed with default settings. You can configure the settings using the script `/opt/hp/hpsmh/sbin/hpSMHSetup.sh` for Itanium systems.
- On Windows operating systems, the installation enables you to configure HP SMH settings during installation.
- On both Windows and Linux operating systems, `smhconfig` allows you to configure the HP SMH security settings.

NOTE: To change the configurations for the Linux and Windows operating systems, see the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

To set up user access and security properly:

1. Add user groups to effectively manage user rights.
2. Configure the trust mode.
3. Configure local or anonymous access.

Signing in

The **Sign In** page enables you to access the **Home** page, which contains the available HP Insight Management Agent.

NOTE: The following warning is displayed on the login screen whenever the certificate or the keys or both are modified:

```
The certificate and keys used by SMH to establish SSL (https) connections
have been replaced. It might have happened because the previous version
was deleted (accidentally or maliciously) or replaced by another
application (HP SIM replaces the certificate and keys when installed
on top of SMH). Please, verify what happened to the previous version
and take the appropriate actions.
```

The **Sign In page** components include:

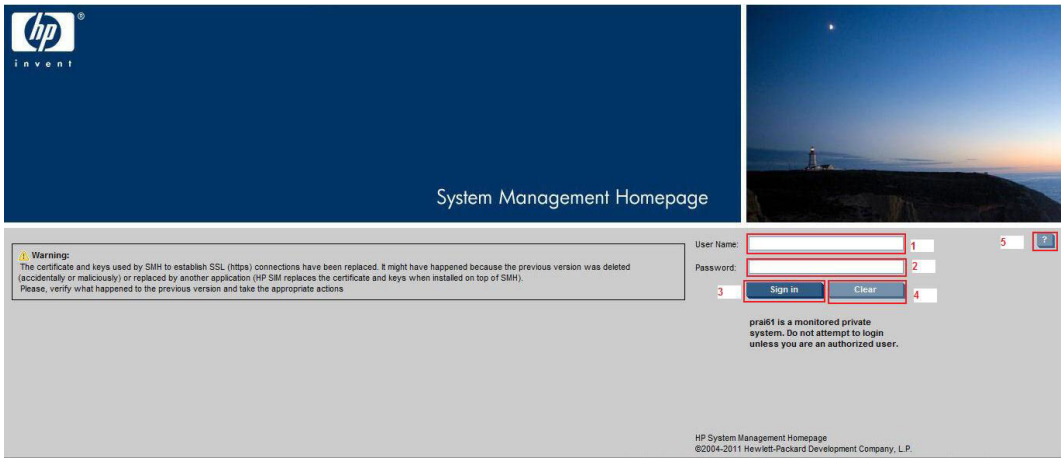
- Two fields to input your user name and password from an account that is part of a valid group configured in the SMH **users groups** configuration article.

NOTE: HP SMH uses the root certificate, intermediate certificate, and the Certificate Root List (CRL) of the certificate to verify the revocation status of trusted certificate used for SSO. If the certificate is found to be revoked or an error is encountered during verification, HP SMH does not allow the user to access HP SMH through SSO and redirects the user to the login page. HP SMH displays the following warning message on the login screen when the SSL certificate is revoked: `Failed to verify CA signed certificate used by SMH. See SMH logs for more details.`

- Two buttons under the input fields:
  - **Sign In**

    Validates the values in the user name and password. If both values are valid, the HP SMH Home page appears.
  - **Clear**

    Erases the input values.
- The question mark icon, **?**, when clicked, displays or hides the tooltip box that displays information about the authentication mechanism and sign-in process.


invent
System Management Homepage
Warning:
The certificate and keys used by SMH to establish SSL (https) connections have been replaced. It might have happened because the previous version was deleted (accidentally or maliciously) or replaced by another application (HP SIM replaces the certificate and keys when installed on top of SMH).
Please, verify what happened to the previous version and take the appropriate actions
User Name:
Password:
Sign in
Clear
1
2
3
4
5
?
prai61 is a monitored private system. Do not attempt to login unless you are an authorized user.
HP System Management Homepage
©2004-2011 Hewlett-Packard Development Company, L.P.

1 **User Name**. The user must be part of a user group accepted by HP SMH.
2 **Password**. The user name and password must match a valid user.
3 **Sign In**. Validates user name and password for signing-in to HP SMH.
4 **Clear**. Erases user name and password input fields.
5 **Question mark**. Show/hide tooltip box.

If an error occurs on a sign-in attempt, you are returned to the **Sign In** page.

A configuration mechanism enables the administrator to customize the image and the message in the **Sign In** page. The administrator can use a custom logo and warning message. As the pages load, HP SMH verifies if the personalized content is enabled and available. If the content is not available, HP SMH uses the standard image and warning message.

Starting HP SMH from Internet Explorer

To sign in to HP SMH with Internet Explorer:

1. Navigate to **`https://hostname:2381/`**.

   The first time you browse to this URI, the **Security Alert** dialog box appears, prompting you to indicate whether to trust the server. If you do not import the certificate, the **Security Alert** appears every time you browse to HP SMH.

   For more information about procedures on changing the configuration variables, see the *HP System Management Homepage Installation Guide* on the HP Technical Documentation Web site at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

   NOTE: To implement your own Public Key Infrastructure (PKI) or install your own generated certificates into each managed system, you can install a certificate authority Root Certificate into each browser to be used for management. If a Root Certificate is implemented, the **Security Alert** dialog box does not appear. If the alert appears, you might have browsed to the wrong system. For more information about installing the **certificate authority Root Certificate**, see the online help in your browser.

2. Click **Yes**.

   The **Sign In** page appears. If you have enabled **Anonymous** access during installation, then System Management Homepage appears.

3. Enter your user name that is recognized by the operating system.

   - **Linux**

     HP SMH initially allows access to users belonging to the root operating system group.

   - **Windows**

     HP SMH allows access to users belonging to the Administrators operating system group.

   If the user credentials cannot be authenticated, the user is denied access.

   After logging into HP SMH as an initially allowed user, use the Security Settings to grant access to users in other operating system groups.

   Administrator on Windows and *root* on Linux have administrator access on HP SMH.

4. Enter the password that is recognized by the operating system.
5. Click **Sign In**.

   The System Management Homepage appears.

Starting HP SMH from Mozilla or Firefox

To sign in to HP SMH with Mozilla or Firefox:

1. Navigate to **`https://hostname:2381/`**.

   For more information about procedures on changing the configuration variables, see the *HP System Management Homepage Installation Guide* on the HP Technical Documentation website at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

2. Click **OK**.

   The **Sign In** page appears. If you have enabled **Anonymous** access during installation, then System Management Homepage appears.

3. Enter your user name that is recognized by the operating system.

   - **Linux**

     HP SMH initially allows access to users belonging to the root operating system group.

   - **Windows**

     HP SMH allows access to users belonging to the Administrators operating system group.

Administrator on Windows and *root* on Linux have administrator access on HP SMH.

4. Enter the password that is recognized by the operating system.
5. Click **Sign In**.

   The System Management Homepage appears.

Starting HP SMH from HP SIM

To start HP SMH by signing in to HP SIM with a Web browser:

1. Navigate to `https://hostname:50000/`.

   The first time you browse to this link, the **Security Alert** dialog box appears, asking if you want to trust the server. If you do not import the certificate, the **Security Alert** appears each time you browse to Systems Insight Manager (HP SIM).

   NOTE: To implement a custom Public Key Infrastructure (PKI) or install your own generated certificates into each managed system, you can install a certificate authority Root Certificate into each browser to be used for management. If a Root Certificate is implemented, the **Security Alert** dialog box does not appear. If the alert appears, you might have browsed to the wrong system. For more information about installing the **certificate authority Root Certificate**, see the online help in your browser.

2. Click **Yes**.

   The **Sign In** page appears.
3. Enter your user name that is recognized by the operating system.
4. Enter the password that is recognized by the operating system.
5. Click **Sign In**.
6. Select **Tools→System Information→System Management Homepage**.
7. Select a target system from the list.
8. Select a check box next to a target system, and then click **Apply**.
9. Verify the target system by selecting a check box next to the system, and then click **Run Now**.

   The **Security Alert** dialog box appears, prompting you to trust the server. If you do not import the certificate, the **Security Alert** appears each time you browse to HP SMH.

   The System Management Homepage appears.

Configuring firewall settings

Windows

Some operating systems including Windows XP with Service Pack 2 and Windows Server 2003 SBS implement a firewall that prevents browsers from accessing the ports required for the Version Control Repository Manager access. To resolve this issue, configure the firewall with exceptions to enable browsers to access the ports used by HP SIM and Version Control Repository Manager.

NOTE: For Windows XP with Service Pack 2, the firewall configuration leaves the default SP2 security enhancements intact, but enables traffic over the ports. These ports are required for the Version Control Repository Manager to run. The secure and insecure ports must be added to enable proper communication with your browser.

To configure the firewall:

1. Select **Start→Settings→Control Panel**.
2. To configure the firewall settings, double-click **Windows Firewall**.
3. Select **Exceptions**.
4. Click **Add Port**.

5. Enter the following product name and the port number information.
   Add the exceptions listed in the following table to the firewall protection:

Table 1 Firewall exceptions

Product	Port Number
HP SMH Insecure Port:	2301
HP SMH Secure Port:	2381

6. Click **OK** to save your settings and close the **Add a Port** dialog box.
7. Click **OK** to save your settings and close the **Windows Firewall** dialog box.

Linux

Configuring firewalls varies, depending on the version of Linux installed.

Red Hat Enterprise Linux 4, 5, and 6

The following displays an example of iptables firewall rules for Red Hat Enterprise Linux 4 and 5 in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80
-j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21
-j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22
-j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

The following displays the new value in the iptables firewall rules for Red Hat Enterprise Linux 4 and 5 that allows access to HP SMH in the `/etc/sysconfig/iptables` file:

```
# Firewall configuration written by redhat-config-securitylevel
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
```

```
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
-A RH-Firewall-1-INPUT -i lo -j ACCEPT
-A RH-Firewall-1-INPUT -p icmp --icmp-type any -j ACCEPT
-A RH-Firewall-1-INPUT -p 50 -j ACCEPT
-A RH-Firewall-1-INPUT -p 51 -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 80
-j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 21
-j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 22
-j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2301
-j ACCEPT
-A RH-Firewall-1-INPUT -m state --state NEW -m tcp -p tcp --dport 2381
-j ACCEPT
-A RH-Firewall-1-INPUT -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

SUSE Linux Enterprise Server

SUSE Linux Enterprise Server 9 and 10 firewalls are configured using the YAST2 utility.

To configure the firewall:

1. Using the YAST2 utility, select **Security & Users→Firewall**.
   The **Firewall Configuration (Step 1 of 4): Basic Settings** window appears.
2. Click **Next**.
   The **Firewall Configuration (Step 2 of 4): Services** window appears.
3. In the **Additional Services** field, enter `2301:2381`, and then click **Next**.
   The **Firewall Configuration (Step 3 of 4): Features** window appears.
4. Click **Next**.
   The **Firewall Configuration (Step 4 of 4): Logging Options** window appears.
5. Click **Next**.
   A dialog box appears asking you to confirm your intention to save settings and active firewall.
6. Click **Continue**.
   The firewall is configured and your settings are saved.

Configuring timeout settings for HP-UX

Two HP SMH timeout settings can be configured:

- **SMH service timeout**

  Sets the amount of time, in minutes, before the HP SMH server stops.

- **SMH session timeout**

  Sets the amount of time, in minutes, before an HP SMH GUI session stops.

NOTE: Selecting the **Session never expires** check box avoids HP SMH session timeouts by sending a background request every three minutes. This option, when selected, also prevents HP SMH service timeouts. **Session never expires** is only available on HP-UX systems.

Configuring SMH Service Timeout

The HP SMH service timeout setting enables you to configure the HP SMH timeout in minutes. If service timeout is not defined or is set to 0 (zero), HP SMH starts without a service timeout. If the service timeout is less than the HP SMH session timeout, HP SMH stops 3 minutes after the HP SMH session timeout.

When the HP SMH **automatic startup on boot** startup mode is used, HP SMH starts without a service timeout.

To modify the service timeout setting, complete the following steps:

1. Copy the existing `/opt/hpsmh/conf/timeout.conf` file into a different directory.
2. Edit the `timeout.conf` file:
   a. Open `/opt/hpsmh/conf/timeout.conf` with a text editor.
   b. Modify the following line to specify a value greater than 9 minutes.

      ```
      TIMEOUT-SMH=30
      ```

   c. Save and close the file.
3. Restart the HP SMH service.

Configuring SMH Session Timeout

The HP SMH session timeout setting enables you to configure the HP SMH GUI timeout in minutes. An HP SMH GUI session is stopped after the session timeout time period elapses without user activity.

If the session timeout is not defined, it is set to 15 minutes.

To modify the session timeout setting, execute the following steps:

1. Copy the existing `smhpd.xml` file into a different directory.

   The file is located in the following path.

   HP-UX

   `/opt/hpsmh/conf.common/smhpd.xml`
2. Edit the `smhpd.xml` file:
   a. Open `smhpd.xml` with a text editor in the following manner.

      `/opt/hpsmh/conf.common/smhpd.xml`

   b. Add the following line between the `<system-management-homepage>` and `</system-management-homepage>` tags:

      `<session-timeout>`*`value`*`</session-timeout>`

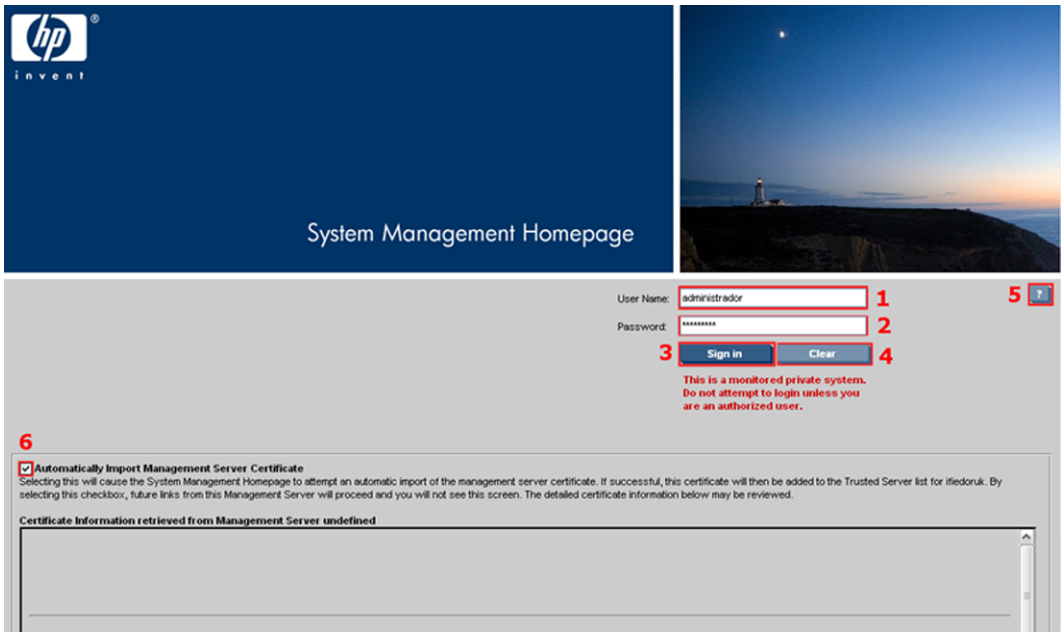
   c. Replace *`value`* with a value between 6 and 120.
   d. Save and close the file.

3. Restart the HP SMH service.

Automatically importing certificates

The **Automatically Import Management Server Certificate** feature enables you to automatically import the HP SIM certificate when accessing the HP SMH from an HP SIM system.

NOTE: Your login must have administrative access to HP SMH to automatically import the HP SIM certificate.



1. **User Name**. The user must be part of a user group accepted by HP SMH.
2. **Password**. The user name and password must match a valid user.
3. **Sign In**. Validates user name and password for signing in to HP SMH.
4. **Clear**. Erases user name and password input fields.
5. **Question mark**. Show/hide tooltip box.
6. **Automatically import management server certificate**. Imports certificate data if checked when the sign in button is pressed.

To automatically import the HP SIM certificate:

1. From an **HP Systems Insight Manager** or **HP Insight Manager 7** system, select a link to a system.

   If the **Trust By Certificate** option is selected in HP SMH **Settings**, click the **Security** link, and then click the **Trust Mode** , and a certificate for the HP SIM system you are accessing has not been imported into the **Trusted Certificates List**, the **Sign In** page displays the **Automatically Import Management Server Certificate** option. The Certificate Information retrieved from *SERVER NAME* displays the HP SIM certificate details.
2. If you do not want to add the HP SIM certificate to the **Trusted Certificates List**; deselect **Automatically Import Management Server Certificate**. Deselecting this option still requires you to enter login credentials. However, administrator credentials are not required to login.

   If you enable HP SMH to automatically import the HP SIM certificate, future access to the system is seamless. You are not prompted for your login credentials.
3. Leave **Automatically Import Management Server Certificate** selected, enter your HP SMH credentials, and then click **Sign In** to automatically import the certificate.

   The certificate is added to the **Trusted Certificates List**.

Signing out

You can sign out of HP SMH, using either of the following options:

- In the HP SMH header, click **Sign Out**.
  The HP System Management Homepage **Sign in** page appears.
- Close every instance of the Web browser used to sign in to HP SMH.

3 Scenarios

IP Binding

You can use IP Binding for example when a system has multiple IP addresses and you want to limit the access to HP SMH to particular networks or subnets like:

- For infrastructure (IPv4 and IPv6)
- Multiple subnets
- Security
- Bandwidth

For more information, see "IP Binding category" (page 31).

IP Restricted Login

IP Restricted Login is useful if you want to:

- Limit remote access to HP SMH to include only specific remote servers
- To exclude entire ranges of remote servers
- Increase security by limiting remote access

For more information, see "IP Restricted Login category" (page 32).

Local Server Certificate

Local server certificate is useful for security reasons through creating self-signed certificates instead of certificates generated by HP.

For more information, see "Local Server Certificate category" (page 34).

Port 2301

For security reasons, you can reduce the amount of open ports in the environment.

For more information, see "Port 2301 category" (page 35).

Kerberos Authentication (Windows only)

Kerberos offers Single Sign-On (SSO) capability on secure networks. In a Kerberos environment, users log in only once at the start of their session, acquiring Kerberos credentials that are used transparently to log in on all other services available, such as SSH, FTP, and authenticated web sessions.

For more information, see "Kerberos Authentication category (Windows only)" (page 41).

User Groups

The user groups feature allows you to manage user access to HP SMH based on operating system level account groups. Operating system account groups can be configured for administration reasons.

For more information, see "User Groups category" (page 44).

Alternative Names (Windows and Linux only)

The alternative names feature simplifies the use of certificates not generated, by HP by enabling HP SMH to recognize DNS names and IP addresses associated with a certificate.

For more information, see "Alternative Names Certificates (Windows and Linux only)" (page 48).

4 Navigating the software

The HP System Management Homepage (HP SMH) displays all HP Web-enabled System Management Software that provides information. In addition, HP SMH displays various categories (in boxes) that have icons defining the status of the items.

The HP SMH main page is divided into two major areas: the header and the standard container.

- **Header Frame**

  The header frame is constantly visible regardless of the page you are viewing and contains the following four subareas:

  - **Master header.** In Windows and Linux, the links show the path you are viewing, the user, and a **Sign Out** link.

  - **Menu.** Each item is a direct link to a page or section including:
    - Home
    - Settings
    - Tasks
    - Tools
    - Logs
    - Webapps
    - Support
    - Help

  - **Main title area.** The area under the master header and menu contains the following items.
    - **Title.**

      The title of the section of page you are viewing.
    - **Host Name.**

      The name of the system.
    - **System Model.**

      The model appears as **Unknown** if the HP Insight Management Agent for servers is not installed on the system.
    - **Management Processor.**

      The name of the management processor.
    - **Icons.**

      An option that enables you to switch between icon and list view modes when clicked.

Data Source

Indicates which source is populating management data. For instance, WBEM for HP Insight Management WBEM Providers or SNMP for HP Insight Management Agents. If no source is installed, no data string will appear.

– **Bread crumbs.**

The area under the main title that is divided into four parts.

– First level menu item

– **Legend.**

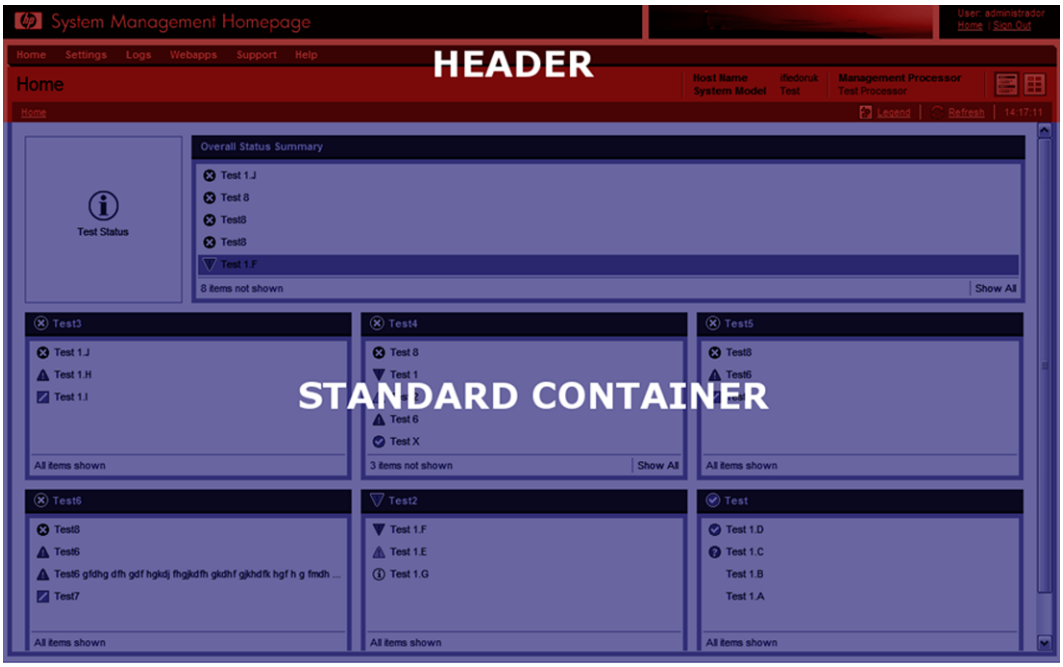
A link that, when clicked, displays a tooltip box listing all possible statuses of webapps.

– **Refresh.**

A link that reloads the header and information areas.

– **Time.**

Displays the time the page was loaded. When you mouse over the time area, you can see the date the page was loaded.



- **Data Frame.**

The standard container contains the sections or pages as:

  - Boxes
  - Icons
  - Pages as configurations
  - Support

- Help
- Webapps

The data frame shows the status for all HP Web-enabled System Management Software and utilities on the system.

Information areas

Depending on your operating system (Linux or Windows), the following information areas appear in the header or data frames:

- **HP SMH Pages**
  - Signing In
  - The Home Page
  - The Settings Page
  - The Tasks Page
  - The Tools Page (HP-UX only)
  - The Logs Page
  - The Installed Webapps Page
  - The Support Page
  - The Help Page
  - **Current User.**

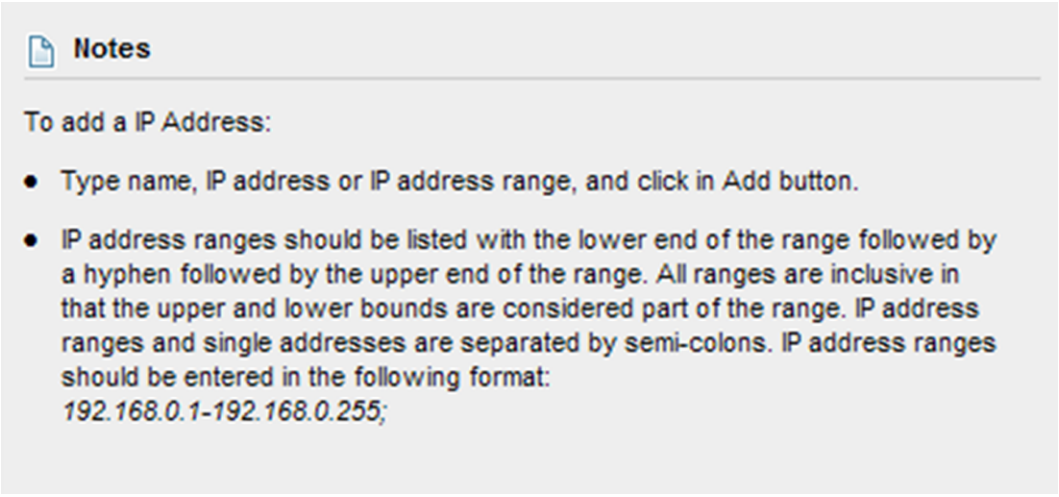
    The Current User displays the identity of the user that is signed in.
    - If the user is a operating system-based user, a **Sign Out** link appears.
    - If anonymous access is enabled, the **Current User** displays **hpsmh_anonymous** and the **Sign In** link appears.
    - If **Local Access** is enabled, the **Current User** displays **hpsmh_local_anonymous** or **hpsmh_local_administrator**, depending on what level of access has been enabled, and local access appears below user type.
    - If user type is **hpsmh_local_administrator**, no sign in or sign out link appears.
  - **Boxes.**

    Boxes display webapps results in a list of items with their result status.
    - An Overall System Health Status icon represents the worst status of items inside the box and appears in the title bar along with the title.
    - Under the title bar, is a list of items in the box. Each item can have a status icon to the left of its name.
    - In the footer of the box, is an expansion line with a link that, when clicked, expands the height of the box to include the total number of items if the items exceed the five-line limit.
  - **Loading screen.**

    When an item is selected, a status indicator appears as the **Loading screen** during the load process of the page. This prevents users from selecting other items after the initial selection.

- **Number of columns.**

  The number of boxes or columns presented in each line in the list view mode is defined by the display resolution setting. For example, if your resolution is set at 800x600, only three boxes are presented in a line, while in greater resolutions, the number of boxes visible is four.


Notes
To add a IP Address:
Type name, IP address or IP address range, and click in Add button.
IP address ranges should be listed with the lower end of the range followed by a hyphen followed by the upper end of the range. All ranges are inclusive in that the upper and lower bounds are considered part of the range. IP address ranges and single addresses are separated by semi-colons. IP address ranges should be entered in the following format:
192.168.0.1-192.168.0.255;

- **Notes.**

  Notes are sections placed on the right side and used in most pages. These notes inform you how to use the controls and what kind of values is expected.

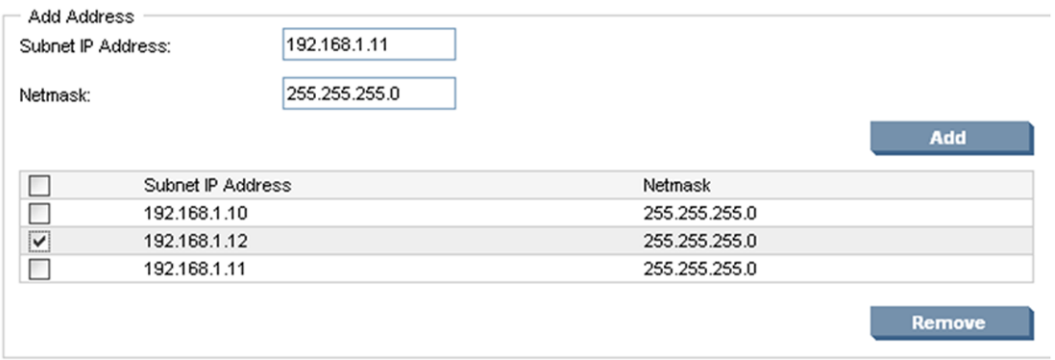
- **Icon view.**

  Icons appear for items and sections. When an icon is clicked, another page appears with its items as icons. You can view the status of the items inside the box by hovering your mouse over the icon to view a tooltip containing the total of **Critical**, **Major**, **Minor** and **Warning** statuses of installed applications.

Your session will expire in 1 minute if you remains inactive.
If you would like to continue with your session, click here to close this warning.

- **Timeout Warnings.**

  Timeout warnings appear as a tooltip box in the page footer on the right side when you do not load a page in SMH within the time limit set for timeouts.



- **Dynamic Lists in Pages.**

  A dynamically created list of elements appears for each item you want to add or remove to a page and are available for the following pages:

  - IP Binding
  - IP Restricted Login
  - Trust Mode
  - Kerberos Authentication
  - User Groups

- **Legend:**

  This link displays a tooltip box that lists the status of the installed webapps.

Table 2 Status icons

Icon	Status
	Critical
	Major
	Minor
	Warning
	Normal
	Disabled
	Unknown
	Informational

- **Management Processor.**

  This displays a link to the **Remote Insight Lights-Out Edition** (**RILOE**) board or the **Integrated Lights-Out** (**iLO**) board. This information is provided by the HP Insight Management Agent. If no HP Web-enabled System Management Software is installed that provides this information, **none** appears.

Icon view

Icons.

An option that enables you to switch between icon and list view modes when clicked.

Table 3 Icon View

Icon	Description
	Component Status Summary The **Component Status Summary** displays links to all subsystems that have a critical, major, minor, or warning status, which the integrated HP Web-enabled System Management Software provides. If there are no agents

Table 3 Icon View *(continued)*

Icon	Description
	installed or no critical, major, minor or warning items, the **Component Status Summary** displays **no items**.
	Generic Icon The generic icon is provided when a webapp does not have an icon.
	System Management Homepage Illustrates sections related to the System Management Homepage.
	Security Options Provides links that enable you to configure HP SMH settings. It provides links to the following: • Anonymous/Local Access • IP Binding • IP Restricted Login • Local Server Certificate • Port 2301 (Windows only) • Port 2301 and AutoStart (Linux Only) • Timeouts • Trust Mode • Trusted Management Servers • Kerberos Authentication (Windows Only) • User Groups
	Anonymous/Local Access Enables the administrator to set options that allow anonymous users to access SMH pages or to allow automatic login to SMH when running in a local console as administrator or anonymous user.
	IP Binding Enables you to control the addresses that SMH is bound to.
	IP Restricted Login Enables you to add addresses from where SMH is accessible or blocked.
	Local Server Certificate This category has two blocks and is used for generation of certificate requests that can be sent to a Certificate Authority (CA) to sign and later import the signed certificate that was received.
	Port 2301 (Windows only) Enables you to configure access to Port 2301.
	Port 2301 and AutoStart (Linux only) Enables you to configure access to Port 2301 and Autostart.

Table 3 Icon View *(continued)*

Icon	Description
	Timeouts Configures the values of timeout for SMH. Two timeouts can be configured: Session timeout and UI timeout.
	Trusted Management Servers Configures the certificates that are stored in the server and allows you to add or remove certificates.
	User Groups Allows an authorized user to configure which group of users has access to HP SMH and their respective access level.
	Kerberos Users Allows an authorized user to configure which users have **Kerberos** authenticated access to HP SMH and their respective access level.
	UI Properties Controls options for the appearance of HP SMH. It has controls for choosing between list and icon view, if you want to use custom text and images relating to your company, and box and item ordering type by name or by status. These options serve as the default options for all users unless users set specific options in **User Preferences**. For more information, see UI Properties category.
	User Preferences Enables you to set how HP SMH appears. It has controls for choosing between list and icon view, and box and item ordering type by name or status. These settings are valid for the user who sets them. These values are stored for 30 days. For more information, see User Preferences category.
	System Management Homepage Logs The **System Management Homepage Log** contains HP System Management Homepage (HP SMH) configuration changes as well as successful and failed sign-in attempts. It is helpful when troubleshooting sign-in or access issues when signing in directly to HP SMH, or from the HP Systems Insight Manager (HP SIM).
	Http error log The **Httpd Error Log** contains error information generated by HP SMH modules, Kerberos misconfiguration errors, and CGI execution errors (httpd). It is the first place to look when a problem occurs with starting the server or with server operation because the log often contains details of what went wrong and how to fix the problem.

HP SMH pages

The HP SMH displays up to nine pages that enable you to access and configure settings related to participating HP Web-enabled System Management Software. The **Tasks** page and the **Tools** page appears if HP Web-enabled System Management Software provides information for them.

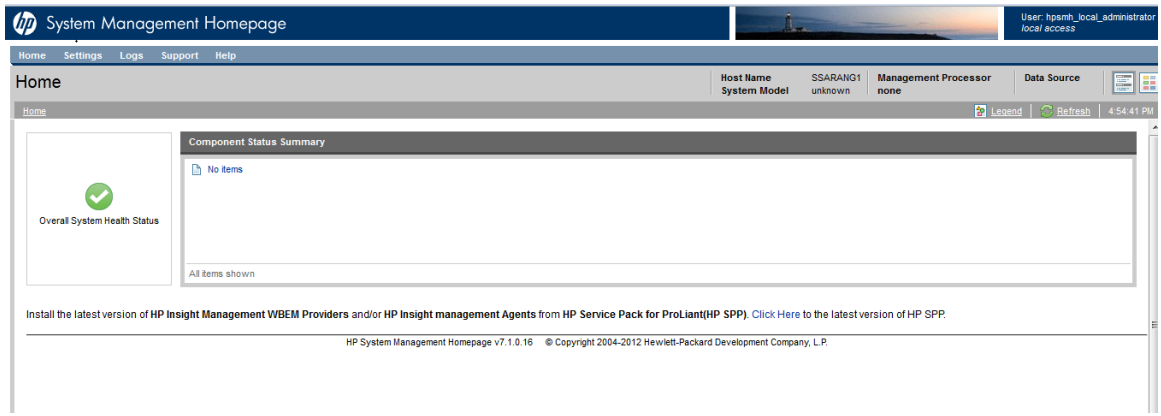
HP SMH pages include:

- “Signing in” (page 7)
- “The Home page” (page 25)
- “The Settings page” (page 26)
- “The Tasks page” (page 50)
- “The Tools page (HP-UX only)” (page 51)
- “The Logs page” (page 52)
- “The Installed Webapps page (Windows and Linux only)” (page 55)
- “The Support page” (page 56)
- The Help page

5 The Home page

The **Home** page provides the system, subsystem, and status views of the server. The **Home** page displays groupings of systems and their status. The information on the **Home** page is provided by the integrated agents or management utilities.

For Linux and Windows operating systems, the **Home** page includes information provided by integrated version control, server, and storage agents.



Component Status Summary

The **Component Status Summary** displays links to all subsystems that have a critical, major, minor, or warning status, which the integrated HP Web-enabled System Management Software provides. If there are no agents installed or no critical, major, minor or warning items, the **Component Status Summary** displays **no items**.

Overall System Health Status

The **Overall System Health Status** displays a status icon with a label below it. A specific webapp sets the value of the **Overall System Health Status** icon using a predefined heuristic to signal the Overall System Health Status. If no webapp sets the Overall System Health Status, the worst of all the statuses in the **Component Status Summary** box is displayed.

6 The Settings page

The **Settings** page contains links to the settings and configuration pages of the HP System Management Homepage (HP SMH) and other integrated management tools found on the **Tools** page.

SNMP webagent box

Provides links that enable you to configure HP Web-enabled System Management Software agents.

- **SMH Data Source category (Windows and Linux only)**

  Sets options for HP SMH Data Source.

- **SNMP Configuration category (Windows and Linux only)**

  Sets options for HP Web-enabled System Management Software agents.

- **UI Options category (Windows and Linux only)**

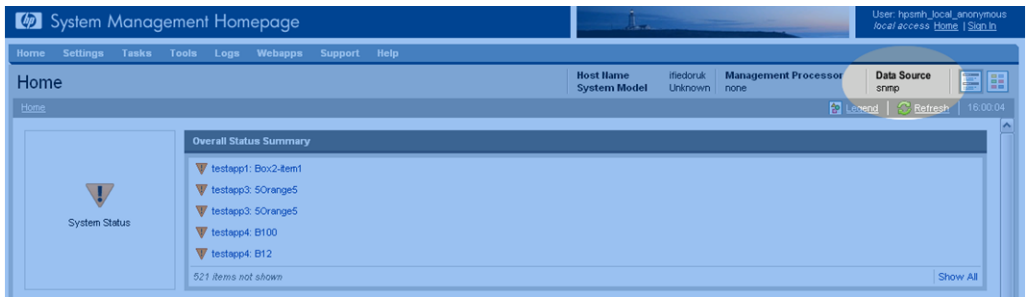
  Sets options for HP Web-enabled System Management Software agents help.

SMH Data Source category (Windows and Linux only)

The **Data Source** page enables you to change the HP SMH management data source.

The **Data Source** setting is only available if the HP Insight Management WBEM providers are installed.

NOTE: If no source is installed, SMH Data Source is shown with no data string.



- **SMH Data source: WBEM**

  Indicates that HP Insight Management WBEM Providers are currently providing management data to the SMH pages for this server.

- **SMH Data source: SNMP**

  Indicates that HP Insight Management Agents (SNMP) are currently providing management data to the SMH pages for this server.

To configure the **Data Source**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **SNMP Webagent** box, click the **Data Source** link.
3. Select **SNMP** or **WBEM** .
4. Click **Save and Apply Changes**.

SNMP Configuration category (Windows and Linux only)

The **SNMP Configuration** page provides web serving and abstracts security and HP SIM interaction for webapps. For more information, see the *HP Systems Insight Manager 5.2 Technical Reference*

Guide, available on the HP Technical Documentation website at http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

To configure the **SNMP Configuration**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **SNMP Webagent** box, click the **SNMP Configuration** link .

UI Options category (Windows and Linux only)

The **UI Options** page enables you to display inline help icons.

To configure the **UI Options**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **SNMP Webagent** box, click the **UI Options** link.
3. Remove the check in the check box beside **Show Help Icons** to no longer display inline help icons.

   Select the check box beside **Show Help Icons** to display the inline help icons.
4. Click **Save and Apply Changes**.

System Management Homepage Box

The System Management Homepage Box provides links that enable you to configure HP SMH settings.

- **UI Properties category**

  Sets options for the appearance of HP SMH.
- **User Preferences category**

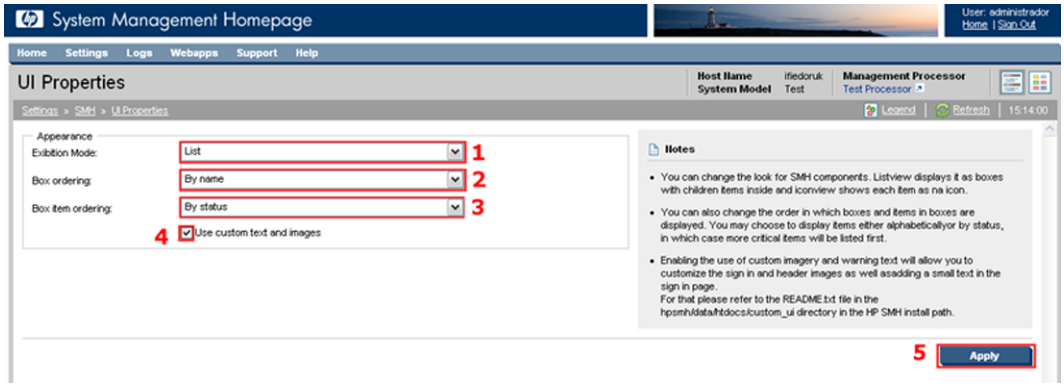
  Sets how HP SMH appears.
- **Security**

  Displays links for setting the security options.

UI Properties category

The **UI Properties** category controls options for the appearance of HP SMH. **UI Properties** has controls for choosing:

- List view
- Icon view
- Box and item ordering type
  - By name
  - By status
- The last option is used by administrators to set custom images for the master header and **Sign In Page** and custom warning text for the **Sign In Page**.


System Management Homepage
User: administrador
Home | Sign Out
Home Settings Logs Webapps Support Help
UI Properties
Host Name
System Model
Management Processor
Test Processor
Settings » SMH » UI Properties
Legend
Refresh
15:14:00
Appearance
Exibition Mode:
List
1
Box ordering:
By name
2
Box item ordering:
By status
3
4
Use custom text and images
Notes
You can change the look for SMH components. Listview displays it as boxes with children items inside and iconview shows each item as na icon.
You can also change the order in which boxes and items in boxes are displayed. You may choose to display items either alphabeticallyor by status, in which case more critical items will be listed first.
Enabling the use of custom imagery and warning text will allow you to customize the sign in and header images as well asadding a small text in the sign in page.
For that please refer to the README.txt file in the hpsmh/data/htdocs/custom_ui directory in the HP SMH install path.
5
Apply

1 Presentation Mode

Enables you to set the default presentation mode by selecting from a list. The **Presentation Mode** has two options: **List View** and **Icon View**.

2 Box Ordering

Determines the order that the boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical) to best (normal).

3 Box Item Ordering

Determines the order that items in boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical), to best (normal).

4 Use Custom text and images

Enables the administrator to set custom warning messages in the **Sign In** page and imagery in the **Sign In** page and master header.

5 Apply

Save page data.

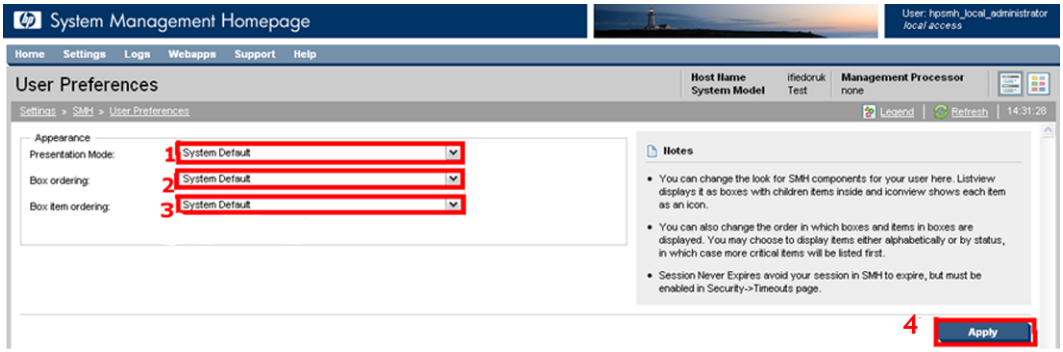
To set **UI Properties**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **UI Properties** link.
3. From the **Presentation Mode** list, Select **List** or **Icon**.
4. From the **Box ordering** list, select **By status** or **By name**.
5. From the **Box item ordering** dropdown list, select either **By status** or **By name**.
6. To use a custom image and custom warning, complete the following steps:
   a. Place the image and text files in the following directories:
      - *SMHBaseDir*`/data/htdocs/custom_ui/logo0.jpg` (for the loading screen image)
      - *SMHBaseDir*`/data/htdocs/custom_ui/logo1.jpg` (for the master header image)
      - *SMHBaseDir*`/data/htdocs/custom_ui/warning1.txt` (for the warning text)

      All three files must be present to view custom images and warning text.
   b. Click the check box beside **Use custom text and images**.
7. Click **Apply**.

User Preferences category

The **User Preferences** category controls options for the appearance of HP SMH.


System Management Homepage
Home
Settings
Logs
Webapps
Support
Help
User Preferences
Host Name
System Model
Management Processor
none
Settings > SMH > User Preferences
Legend
Refresh
Appearance
Presentation Mode:
System Default
Box ordering:
System Default
Box item ordering:
System Default
1
2
3
4
Notes
You can change the look for SMH components for your user here. Listview displays it as boxes with children items inside and iconview shows each item as an icon.
You can also change the order in which boxes and items in boxes are displayed. You may choose to display items either alphabetically or by status, in which case more critical items will be listed first.
Session Never Expires avoid your session in SMH to expire, but must be enabled in Security->Timeouts page.
Apply

1 Presentation Mode

Enables you to set the default presentation mode by selecting from a list. The **Presentation Mode** has two options: **List View** and **Icon View**.

2 Box Ordering

Determines the order that the boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical) to best (normal).

3 Box Item Ordering

Determines the order that items in boxes are shown. If you order by name, the items appear alphabetically. If you order by status, items appear from worst (critical), to best (normal).

4 Apply

Save page data.

To set **User Preferences**, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **User Preferences** link.
3. From the **Presentation Mode** list, select **List** or **Icon**.
4. From the **Box ordering** list, select **By status** or **By name**.
5. From the **Box item ordering** list, select **By status** or **By name**.
6. If you do not want the session to expire (in the case of HP-UX only), click the check box beside **Session Never Expires**.
7. Click **Apply**.

NOTE: Each user is able to set their preferences for a session. Individual user preferences take precendence over settings in UI properties.

Security

The **Security** link provides options for you to manage the security of HP SMH:

- "Anonymous/Local Access category" (page 30)
- "IP Binding category" (page 31)
- "IP Restricted Login category" (page 32)
- "Local Server Certificate category" (page 34)
- "Port 2301 category" (page 35)
- "Timeouts category" (page 37)
- "Trust Mode category" (page 38)

- "Trusted Management Servers category" (page 41)
- "Kerberos Authentication category (Windows only)" (page 41)
- "User Groups category" (page 44)
- "Handling (proper) of the HP SMH certificate revocation" (page 47)
- "Detecting and handling memory leak at runtime (Windows only)" (page 48)

To access Security, select **Settings** from the menu, and then click the **Security** link in the **System Management Homepage** box.

Anonymous/Local Access category

Anonymous/Local access enables you to select the following settings to include:

- **Anonymous Access**

  (Disabled by default). Enabling **Anonymous Access** enables a user to access the HP SMH without logging in. If **Anonymous** is selected, any user, local or remote, has access to unsecured pages without being challenged for a username and password.

  Caution: HP does not recommend the use of anonymous access.

- **Local Access**

  (Disabled by default). Enabling **Local Access** means you can gain local access to HP SMH without being challenged for authentication. This means that any user with access to the local console is granted full access if **Administrator** is selected.

  Caution: HP does not recommend the use of local access unless your management server software enables it.

System Management Homepage
User: administrador
Home | Sign Out
Home Settings Logs Webapps Support Help
Anonymous/Local Access
Host Name ifiedoruk
System Model Test
Management Processor
Test Processor
Settings » SMH » Security » Anonymous/Local Access
Legend
Refresh
15:31:11
Anonymous Access
1 Allow Anonymous users access to unsecured pages
Local Access
2 Turn on automatic logon in System Management Homepage
3 Anonymous
4 Administrator
Notes
When you check to allow Anonymous users acess to unsecured pages, note that this include local users.
When you turn on automatic logon in System Management Homepage, any user with access to the local console will be granted full access if Administrator is selected, without being challenged for a username and password.
5
Apply

1 Allow Anonymous users access to unsecured pages.

2 Turn on automatic logon in HP System Management Homepage

3 **Anonymous Access**

Enables a user to access the HP SMH without logging in. If **Anonymous** is selected, any user, local or remote, has access to unsecured pages without being challenged for a username and password.

4 Enables a Administrator to access the HP SMH without logging in.

5 **Apply**

Save page data.

To enable anonymous access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.

3. Click the **Anonymous/Local Access** link.
4. Under **Anonymous Access**, select the box beside **Allow Anonymous users access to unsecured pages**.
5. Click **Apply** to apply your settings.

To disable anonymous access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Anonymous Access**, remove the check from the box beside **Allow Anonymous users access to unsecured pages**.
5. Click **Apply** to apply your settings.

To enable local access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Local Access**, select the box beside **Turn on automatic logon in System Management Homepage**.
5. Select **Anonymous** or **Administrator**.
6. Click **Apply** to apply your settings.

To disable local access:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Anonymous/Local Access** link.
4. Under **Local Access**, deselect the box beside **Turn on automatic logon in System Management Homepage**.
5. Click **Apply** to apply your settings.

IP Binding category

IP Binding specifies the IP addresses that HP SMH accepts requests from and controls the nets and subnets that requests are processed.

Administrators can configure HP SMH to only bind to addresses specified in the **IP Binding** window. Five subnet IP addresses and netmasks can be defined.

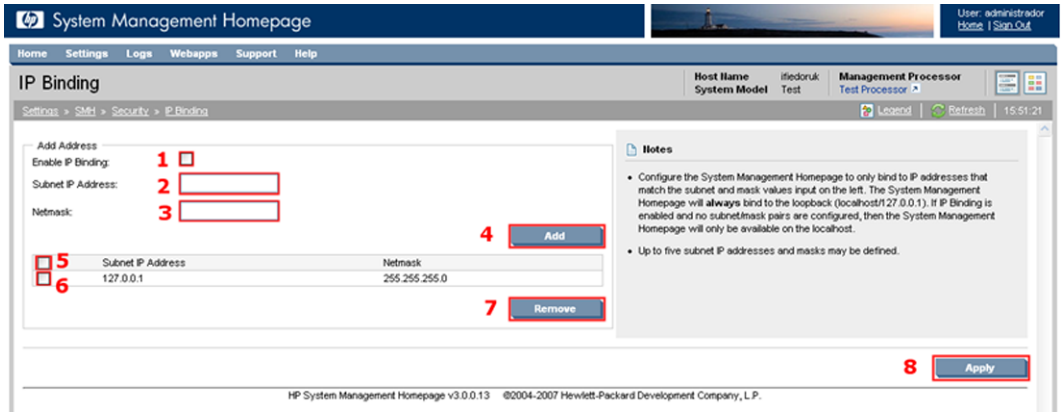
An IP address on the server is bound if it matches one of the entered IP Binding addresses after the mask is applied.

HP SMH on Windows and Linux supports both IPv4 and IPv6 addresses.

For example, If the subnet IP address is 172.24.37.88 and netmask is 255.255.255.0, it means requests are considered from all IP addresses 172.24.37.x (where, x is any value from 1-255).

Similarly, for other netmask values, 255.255.0.0 and 255.0.0.0 IP addresses get bound accordingly. Applying 255.255.255.255 netmask results in binding only a single IP address.

NOTE: HP SMH always binds to 127.0.0.1. If IP Binding is enabled and no subnet/mask pairs are configured, HP SMH is only available to 127.0.0.1. If IP Binding is not enabled, you bind to all addresses.


System Management Homepage
User: administrador
Home | Sign Out
Home Settings Logs Webapps Support Help
IP Binding
Host Name ifiedoruk
System Model Test
Management Processor
Test Processor
Settings » SMH » Security » IP Binding
Legend | Refresh | 15:51:21
Add Address
Enable IP Binding:
Subnet IP Address:
Netmask:
1
2
3
4
Add
5
6
Subnet IP Address
Netmask
127.0.0.1
255.255.255.0
7
Remove
Notes
Configure the System Management Homepage to only bind to IP addresses that match the subnet and mask values input on the left. The System Management Homepage will always bind to the loopback (localhost/127.0.0.1). If IP Binding is enabled and no subnet/mask pairs are configured, then the System Management Homepage will only be available on the localhost.
Up to five subnet IP addresses and masks may be defined.
8
Apply
HP System Management Homepage v3.0.0.13 ©2004-2007 Hewlett-Packard Development Company, L.P.

1 **Enable Binding**

When checked, indicates that binding will be used.

2 **Subnet Address**

Valid address.

3 **Netmask**

Valid netmask.

4 **Add**

Adds the combined IP and Netmask address to the list.

5 **Check All**

Check/uncheck all items in the list of addresses.

6 **Checkbox**

Multiple addresses/names.

7 **Remove**

Remove all checked items from the list.

8 **Apply**

Save all items in the address list.

To configure IP Binding:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Binding** link.
4. Enter the **Subnet IP Address**.
5. Enter the **Netmask**.
6. Click **Add** to add the **Subnet IP Address** and **Netmask** that were entered in the preceding steps.

   You can add up to five subnet IP addresses and netmasks by repeating steps 4 through 7.
7. Click **Apply** to apply the configurations.

NOTE: The netmask is applicable only for IPv4 addresses.

To remove IP addresses from the list:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Binding** link.
4. Select the check box beside the IP address you want to remove.
5. Click **Remove**.
6. Click **Apply** to apply the configurations.

Each IP address and netmask must consist of four octets with values between 0 and 255 (the same for each netmask).

Netmasks must start with the number 1 in the highest bit and continue with all number 1s until they switch to all number 0s (for example, 255.255.0.0, 192.0.0.0, 255.192.0.0).

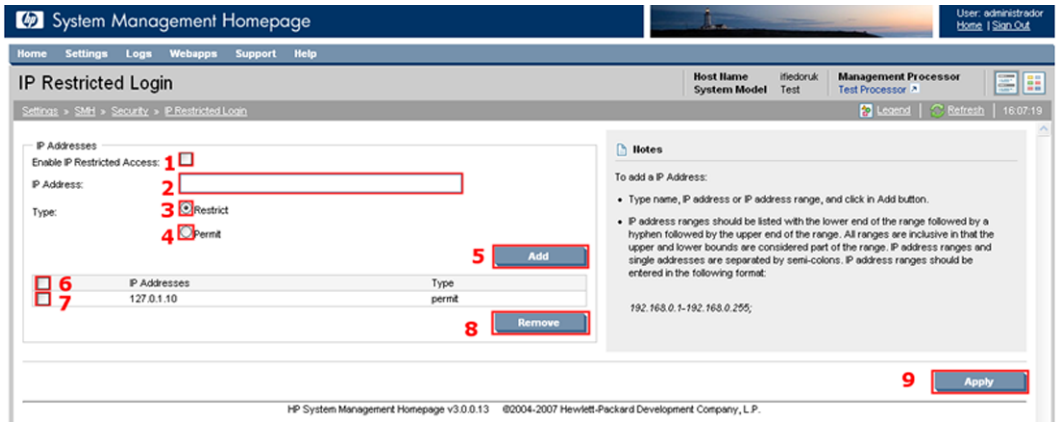
IP Restricted Login category

IP Restricted login enables HP SMH to restrict login access based on the IP address of a system from which the sign-in is attempted.

For Linux and Windows, you can set a restricted address at installation. From all operating systems, administrators can set a restricted address from the **IP Restricted login** page. Note the following:

- If an IP address is restricted, it is restricted even if it is also listed in the permitted box.
- If IP addresses are in the permitted list, only those IP addresses can sign in, except for *localhost*.
- If no IP addresses are in the permitted list, sign in access is allowed to any IP addresses not in the restricted list.

HP SMH on Windows and Linux supports IPv4 and IPv6 addresses.


System Management Homepage
Home
Settings
Logs
Webapps
Support
Help
IP Restricted Login
Host Name
System Model
Management Processor
Test Processor
Legend
Refresh
IP Addresses
Enable IP Restricted Access:
IP Address:
Type:
Restrict
Permit
Add
IP Addresses
Type
127.0.1.10
permit
Remove
Notes
To add a IP Address:
Type name, IP address or IP address range, and click in Add button.
IP address ranges should be listed with the lower end of the range followed by a hyphen followed by the upper end of the range. All ranges are inclusive in that the upper and lower bounds are considered part of the range. IP address ranges and single addresses are separated by semi-colons. IP address ranges should be entered in the following format:
192.168.0.1-192.168.0.255;
Apply
HP System Management Homepage v3.0.0.13 ©2004-2007 Hewlett-Packard Development Company, L.P.

1 **Enable IP Restricted Access**

When checked, indicates that IP restricted login is enabled.

2 **IP Address**

Valid address.

3 **Restrict**

Radio button when selected, restricts IP address login.

4 **Permit**

Radio button when selected, permits IP address login.

5 **Add**

Adds the IP address to the list.

6 **Check All**

Check/Uncheck all items in the list of addresses.

7 **Checkbox**

Multiple addresses.

8 **Remove**

Remove all checked items from the list.

9 **Apply**

Save all items in the address list.

To restrict IP addresses:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **IP Restricted Login** link.
4. Enter the **IP address** or **IP address range**.

   List IP address ranges beginning with the lower end of the range, followed by a hyphen, followed by the upper end of the range. The upper and lower bounds are considered part of the range.

   IP address ranges and single addresses are separated by semicolons. IP address ranges for IPv4 should be entered in the format: 192.168.0.1-192.168.0.255. IP address ranges for IPv6 should be entered in the format: 2001:db8:c18:1:4c7d:fa25:ccf8:d30c-2001:db8:c18:1:4c7d:fa25:ccf8:d30f
5. Select the **Restrict** or **Permit** radio button.
6. Click **Add** to add the configurations.
7. Click **Apply** to apply the configurations.

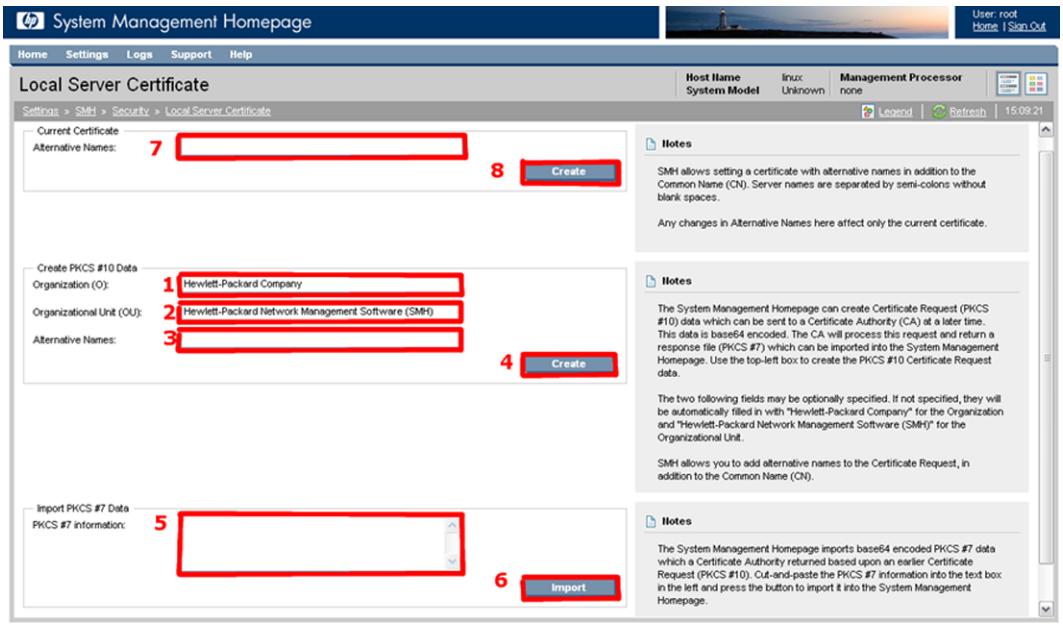
To remove IP addresses from the list:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.

3. Click the **IP Restricted Login** link.
4. Select the check box beside the IP addresses you want to remove.
5. Click **Remove**.
6. Click **Apply** to apply the configurations.

Local Server Certificate category

The **Local Server Certificate** link enables you to use certificates that are not generated by HP.



1 **Organization (O)**

The name of the organization.

2 **Organizational Unit (OU).**

The name of the unit within the organization requesting the certificate.

3 **Alternative Name**

4 **Create**

Create the certificate request.

5 **PKCS #7 Information**

PKCS #7 fields filled.

6 **Import**

Import the signed certificate.

7 **Alternative Names**

Valid server name list.

8 **Create**

Re-create the certificate adding the given alternative names.

If you use the following process, the self-signed certificate that was generated by the HP SMH is replaced with one issued by a certificate authority (CA).

- The first step of the process is to cause the HP SMH to create a **Certificate Request (PKCS #10)**. This request uses the original private key associated with the self-signed certificate and generates data for the certificate request. The private key never leaves the server during this process.
- After the Public Key Infrastructure **PKCS #10** data is created, the next step is to send it to a certificate authority. Follow your company policies for sending secure requests for and receiving secure certificates.
- After the certificate authority returns the **PKCS #7** data, the final step is to import this into HP SMH.
- After the **PKCS #7** data is imported, the original `\hp\sslshare\cert.pem` certificate file for Windows and `/opt/hp/sslshare/cert.pem` (`/etc/opt/hp/sslshare/cert.pem` in HP SMH 2.1.3 and later on Linux x86 and x86-64) is overwritten with the system certificate from the **PKCS #7** data envelope. The same private key is used for the new imported certificate

that was used with the previous self-signed certificate. This private key is randomly generated at startup when no key file exists.

To create a certificate:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Local Server Certificate** link.
4. Replace the default values in the **Organization** or **Organizational Unit** fields in the **Create PKCS #10 Data** box with your values, up to 64 characters.

   If not specified, they are filled in with *Hewlett-Packard Company* for the **Organization** and *Hewlett-Packard Network Management Software (SMH)* for the **Organizational Unit**.
5. Click **Create** in the **Create PKCS #10 Data** box.

   A screen appears indicating that the **PKCS #10 Certificate Request** data has been generated and stored in `/etc/opt/hp/sslshare/req_cr.pem` on Linux x86 and x64, and *systemdrive:* `\hp\sslshare\req_cr.pem` for Windows.
6. Copy the certificate data.
7. Use a secure method to send **PKCS #10** certificate request data to a certificate authority, request the certificate request reply data in **PKCS #7** format, and request that the reply data is in Base64-encoded format.

   If your organization has its own Public Key Infrastructure (PKI) or Certificate Server implemented, send the **PKCS #10** data to the CA manager and request the **PKCS #7** reply data.

   NOTE: A third-party certificate signer generally charges a fee.
8. When the certificate signer sends the **PKCS #7** encoded certificate request reply data to you, copy this data from the **PKCS #7** certificate request reply and paste it into the **PKCS #7 information** field in the **Import PKCS #7 Data** box.
9. Click **Import**.

   A message appears indicating whether the customer-generated certificate was imported.
10. Restart HP SMH.
11. Browse to the managed system that contains the imported certificate.
12. When prompted by the browser, select to view the certificate and verify that signer is listed as the signer you used, and not HP, before importing the certificate into your browser.

    If the certificate signer you choose sends you a certificate file in Base64-encoded form instead of **PKCS #7** data, copy the Base64-encoded certificate file to `/etc/opt/hp/sslshare/cert.pem` on Linux x86 and x64, and *systemdrive*`:\hp\sslshare\cert.pem` for Windows; then restart HP SMH.

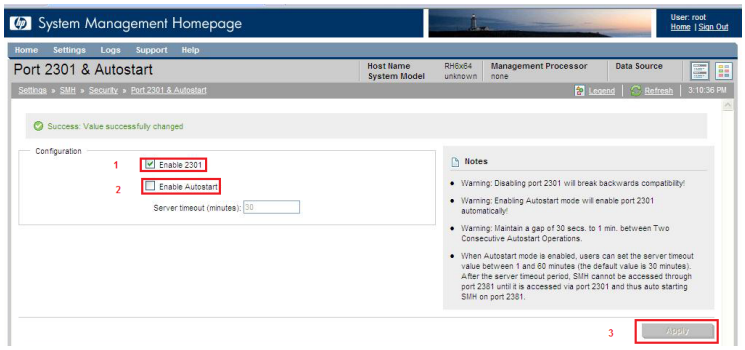
Port 2301 category

The Port 2301 on Windows and Linux systems provide different functionality.

- Port 2301 and Autostart (Linux only)
- Port 2301 (Windows only)

Port 2301 and Autostart (Linux only)

The **Port 2301 and Autostart** link provides options to enable or disable **Port 2301 and Autostart**. The default value for port 2301 is enabled and for Autostart is disabled, preserves the compatibility with HP Web-enabled System Management Software.



1 Enable Port 2301

Sets Port 2301 as enabled or disabed.

2 Enables Autostart mode.

Sets Port 2301 as enabled or disabed.

3 Apply

Record the option into the XML configuration file.

To enable or disable Port 2301, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Port 2301 and Autostart** link.
4. To enable Port 2301, check **Port 2301** check box. To disable Port 2301, clear the **Port 2301** check box.
5. To enable Autostart mode, check **Autostart** check box. To disable Autostart mode, uncheck **Autostart** check box.

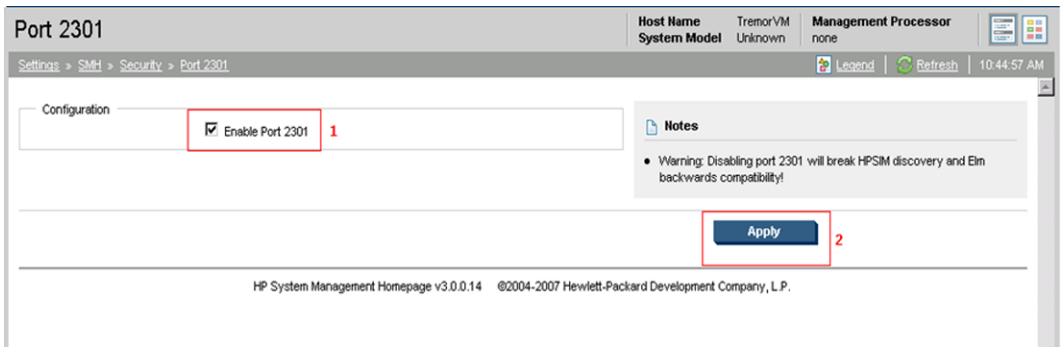
NOTE: Enabling the Autosart mode, enables port 2301 automatically, if it is disabled.

NOTE: Enabling Autostart mode enables server timeout (in minutes) text box which provides you with the option to set the server timeout duration, value between 0 and 60. The default timeout value is 30 minutes.

6. Click **Apply**.

Port 2301 (Windows only)

The **Port 2301** link provides options to enable or disable **Port 2301**. The default value, enabled, which preserves the compatibility with HP Web-enabled System Management Software.



1 Enable Port 2301

Sets Port 2301 as enabled or disabed.

2 Apply

Record the option into the XML configuration file.

IMPORTANT: Consider the following before you disable port 2301:

If you disable port 2301 when HP SMH is in autostart URL mode, the start mode automatically changes to start on boot mode.

To disable Port 2301, complete the following steps:

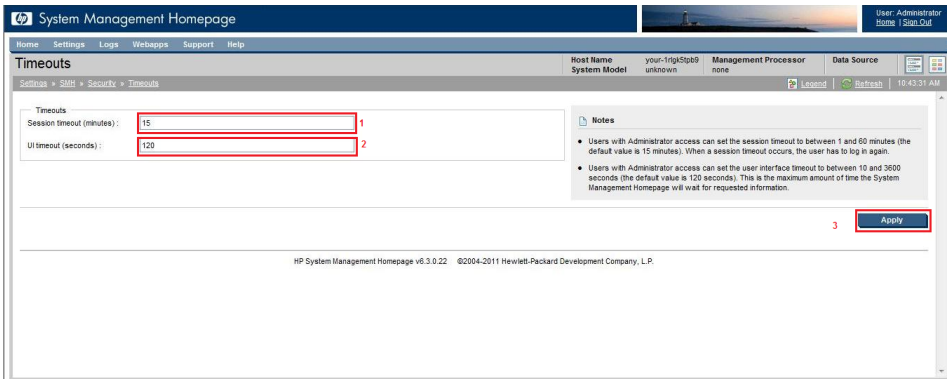
1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Port 2301** link.
4. In the **Configuration box**, clear the **Enable Port 2301** check box.
5. Click **Apply**.

To enable Port 2301, complete the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Port 2301** link.
4. In the **Configuration box**, select the **Enable Port 2301** check box.
5. Click **Apply**.

Timeouts category

The **Timeouts** link provides options to configure the values of the **Session timeout** and **UI timeout**.


System Management Homepage
Home
Settings
Logs
Webapps
Support
Help
Timeouts
Host Name
System Model
Management Processor
Data Source
Legend
Refresh
Timeouts
Session timeout (minutes) :
15
1
UI timeout (seconds) :
120
2
Notes
Users with Administrator access can set the session timeout to between 1 and 60 minutes (the default value is 15 minutes). When a session timeout occurs, the user has to log in again.
Users with Administrator access can set the user interface timeout to between 10 and 3600 seconds (the default value is 120 seconds). This is the maximum amount of time the System Management Homepage will wait for requested information.
3
Apply
HP System Management Homepage v6.3.0.22 ©2004-2011 Hewlett-Packard Development Company, L.P.

1 **Session timeout**: The **session timeout** value represents the amount of time in minutes that a user can remain inactive in an SMH session. Users with Administrator access can set the **session timeout** to between 1 and 60 minutes. The default value is 15 minutes. If a user logs in and remains inactive for an amount of time greater than that specified by **session timeout**, the user is redirected to the **Sign In** page in their next interaction with the user interface.

2 **UI timeout**: The **UI timeout** value represents the maximum amount of time in seconds that the SMH user interface (UI) waits for data requested from webapps. Users with Administrator access can set the **UI timeout** to between 10 and 3600 seconds. The default value is 120 seconds.

3 **Apply**:

Records the chosen values into the XML configuration file.

The following table presents the range of values available for timeouts, with their respective units:

Table 4 Timeout settings

Timeout	Range
Session timeout	1 – 60 minutes (Windows and Linux)
UI timeout	10 – 3600 seconds

Session Timeout

To change the value for Session timeout, complete the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Timeouts** link.
4. In the **Session timeout (minutes)** textbox, enter a value between 1 and 60 minutes in the case of Windows and Linux.
5. Click **Apply**.

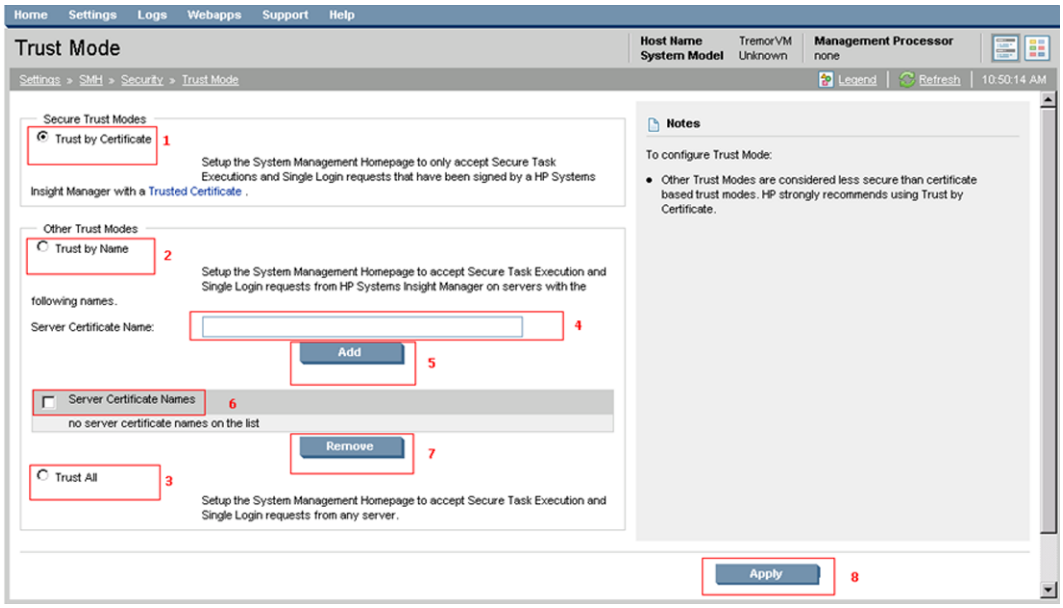
UI Timeout

To change the value for UI timeout, complete the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Timeouts** link.
4. In the **UI timeout (seconds)** textbox, enter a value between 10 and 3600 seconds.
5. Click **Apply**.

Trust Mode category

The **Trust Mode** link provides options to enable you to select the security required by your system. Some situations require a higher level of security than others. Therefore, you have the following security options:



1 **Trust by Certificate**: Sets HP SMH to accept configuration changes only from HP SIM servers with trusted certificates. This mode requires the submitted server to provide authentication by means of certificates. This mode is the strongest method of security because it requires certificate data and

4 **Server Certificate Name**

When a server certificate name is entered, it checks if the server name:

- Is valid (a maximum of 64 characters)
- Contains invalid characters
- Is already in the list

5 **Add**

7 **Remove**

Removes the selected server names from the list.

8 **Apply**

Records the registers in to the XML configuration file.

verifies the digital signature before allowing access. If you do not want to enable remote configuration changes, leave **Trust by Certificate** selected, and leave the list of trusted systems empty by not importing certificates.

This is the default behavior on Linux Itanium.

HP strongly recommends using this option because it is more secure.

2. **Trust by Name**: Sets HP SMH to accept configuration changes only from servers with HP SIM names designated in the **Trust By Name** field. For example, you might use this option if you have a secure network with two groups of administrators in two divisions. It prevents one group from installing software to the wrong system. This option verifies only the HP SIM server that you designate.

   HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

3. **Trust all**

   Sets HP SMH to accept specific configuration changes from systems. For example, you could use the Trust All option if you have a secure network, and everyone in the network is trusted.

   HP strongly recommends using the **Trust by Certificate** option because the other options are less secure.

Add the server name to the list.

6. **Server Certificate Name Enable All**

   Checks all listings in the register's checkboxes.

Configuring Trust Mode

For Linux, the imported HP SMH certificates are stored in the `/opt/hp/hpsmh/certs` directory.

For Windows, the imported HP SIM certificates are stored in the *`systemdrive:`* `\hp\hpsmh\certs` directory.

You must have administrative authority to access this directory.

To trust by certificate:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link .
3. Click the **Trust Mode** link.
4. In the **Secure Trust Modes** box, click the **Trust by Certificate** radio button.

   Choosing this option sets up the HP SMH to accept **Secure Task Executions** and **Single Sign On** requests that are signed by a HP SIM with a **Trusted Certificate**.
5. Click **Apply**.

To trust by name:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trust Mode** link.
4. In the **Other Trust Modes** box, click the **Trust by Name** radio button.
5. In the **Server Certificate Name** textbox, enter the Server Certificate Name.
6. Click **Add**.

   When you click **Add**, the **Server Certificate Name** is validated to see if it meets the following criteria:

   - Each HP SIM server's certificate name must be less than 64 characters
   - The following invalid characters are not included: ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , |
   - The Server Certificate Name is not already in the list

   If the validation test accepts the value, **Server Certificate Name** is added as a new line in the list table. You can add as many as five **Server Certificate Names** by following steps 5 and 6. If you enter more than five certificate names, you receive the alert `No more names can be added`.
7. Click **Apply** to save the configurations.

   Choosing this option sets up HP SMH to only accept **Secure Task Executions** and **Single Sign On** requests from HP SIM on servers with names listed.

To remove a Server Certificate Name from the list, complete the following steps:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trust Mode** link.
4. In the **Other Trust Modes** box, find the **Server Certificate Name** to remove and click the check box beside that name.
5. Click **Remove**.
6. Click **Apply**.

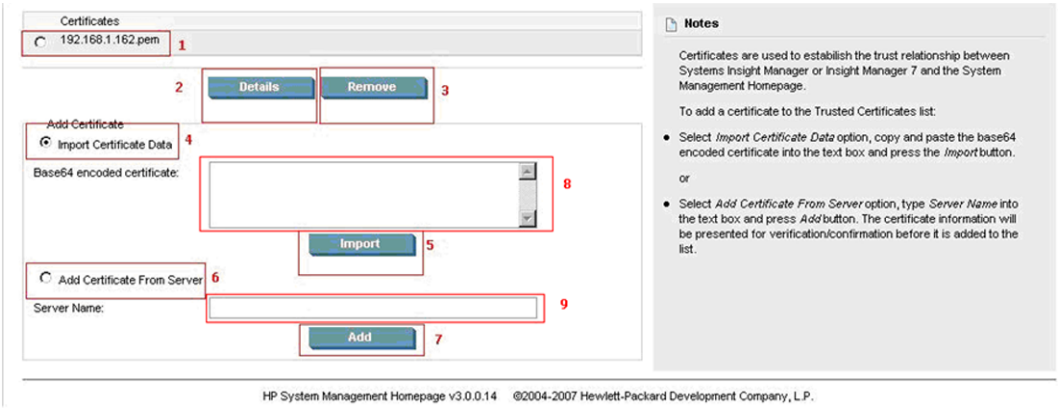
To trust all servers:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trust Mode** link.
4. In the **Other Trust Modes** box, click the **Trust All** button.
5. Click **Apply**.

   Choosing the **trust all** option sets HP SMH to accept **Secure Task Execution** and **Single Sign On** requests from any HP SIM server.

Trusted Management Servers category

Certificates establish the trust relationship between HP SIM or Insight Manager 7 and HP SMH. The **Trusted Management Servers** link enables you to manage your certificates in the **Trusted Certificates List**. Note the following:



To import a certificate to the trusted certificates list:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trusted Management Servers** link.
4. In the **Add Certificate** area, click the **Import Certificate Data** radio button.
5. Copy and paste the Base64-encoded certificate into the textbox.
6. Click **Import**.

To add a certificate from a server:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Trusted Management Servers** link.
4. In the **Add Certificate From Server** area, click the **Add Certificate From Server** radio button.
5. In the **Server Name** textbox, enter the IP address or server name of the HP SIM server.
6. Click **Add**.

Kerberos Authentication category (Windows only)

Kerberos is a trusted third-party network authentication protocol for client/server applications by using secret-key cryptography developed at MIT. **Kerberos** allows different hosts and users to authenticate and confirm the identity of each other.

One primary use of Kerberos is for offering Single Sign-On (SSO) capability on secure networks. Usually in a **Kerberos** environment users log in only once at the start of their sessions, acquiring **Kerberos** credentials that are used transparently to log in on all other services available, such as SSH, FTP, and authenticated web sessions.

A Kerberos domain is a realm and is expressed in all capital letters. For example, the **Kerberos** realm for smhkerberos.com is *SMHKERBEROS.COM*.

Principals are users and services/hosts that are present in a **Kerberos** realm and are allowed to authenticate to each other. A user has a principal name such as `group@REALM` (for example, `joe@SMHKERBEROS.COM`), and a service has a principal name like `service/FQDN@REALM` (for example, `HTTP/box.smhkerberos.com@SMHKERBEROS.COM` or `host/box.smhkerberos.com@SMHKERBEROS.COM`).

Kerberos Authentication Procedure

The following outlines the process when a user accesses secure services in a **Kerberos** realm.

The process only occurs when the user initially logs in to a **Kerberos** realm and tries to perform the first access to a Kerberos-secured service.

1. The user logs in to the system (client) using his or her domain username and password.
2. The user's password is hashed, and this hash becomes the user's secret key.
3. When the user tries to access a service, a message informs the AS that the user wants to access that service.
4. If the user is in the AS database, two messages are sent back to the client:
   a. A Client/TGS session key is encrypted with the user's secret key, which is used in the communication with the TGS.
   b. A Ticket-Granting Ticket (TGT) is encrypted with the secret key of the TGS. A **ticket** is used in **Kerberos** to prove one's identity. The TGT allows the client to obtain other tickets for communication with network services.
5. Upon receiving these two messages, the client decrypts the message containing the Client/TGS session key.

The following process occurs every time a user wants to authenticate to a service:

1. When the user requests a service, the client sends two messages to the TGS:
   - A message composed of the TGT and the requested service
   - An authenticator, is made up of the client's ID and the current timestamp encrypted with the Client/TGS session key received before

   Timestamps are used in **Kerberos** to avoid replication attacks. The clock skew among machines cannot exceed a specific limit.
2. The TGS decrypts the authenticator and sends two new messages back to the client:
   - The client-to-server ticket received from the TGS
   - Another authenticator, made up of the client's ID and the current timestamp, encrypted with the client/server session key
3. The service decrypts the client-to-server ticket with its own secret key and sends the client a message with the received timestamp plus one, confirming its true identity. This message is encrypted with the client/server session key.
4. The client decrypts the message and checks the timestamp. If it is correct, requests may be issued to the service and it sends responses back as expected.

HP SMH Kerberos Authentication

HP SMH provides **Kerberos** Single Sign-On (SSO), allowing users in a **Kerberos** realm to log in without entering a user name and password in the **Sign In** page. If an allowed user accesses HP SMH and has valid **Kerberos** credentials, the **Home** page appears inside HP SMH.

Kerberos authentication is done using the special `URL /proxy/Kerberos` in HP SMH. By accessing the URL, SMH looks for **Kerberos** credentials in the request and perform user authentication.

If the user does not have valid **Kerberos** credentials or if an error occurs during the authentication process, the **Sign In** page appears, showing an error message. For example, if the clock skew among the machines involved in authentication is too large, you receive an error message and are taken to the **Sign In** page.

Kerberos authentication does not work on the following local access situations:

- Accessing HP SMH from the machine where the KDC (AD) is installed
- Accessing HP SMH from the machine where HP SMH is installed

When an authentication error occurs, the system administrator should check the SMH HTTP server error log to obtain more information about the error.

For example, when the clock skew among the machines is too large, the following log message is written: `Thu Jun 25 16:55:09 2009] [error] client 2001:db8:c18:1:b8ca:fcdf:d49d:b5c6] mod_spnego: Kerberos SSO (QueryContextAttributes) failed; SSPI: The function requested is not supported\r\n(-2146893054).`

The following levels of user authorizations are available:

- **Administrator**

  Users with **Administrator** access can view all information provided through HP SMH. The appropriate default user group, *Administrators* for Windows operating systems and and the root user on Linux operating systems always has administrative access.

- **Operator**

  Users with **Operator** access can view and set most information provided through HP SMH. Some web applications limit access to the most critical information to administrators only.

- **User**

  Users with **User** access can view most information provided through HP SMH. Some web applications restrict viewing of critical information from individuals with **User** access.

To enable or disable **Kerberos** and add groups to the allowed **Kerberos** group list, complete the following steps for each level of access.

Kerberos support is provided on a per-user basis.

Kerberos Administrator

To add a **Kerberos** Administrator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. In the **Kerberos Configuration** area, select the box beside **Enable Kerberos Support**.
5. In the **Group Name** textbox, enter a name in the *group@REALM* format or *REALM\group*

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
6. Click the **Administrator** radio button beside **Type**.
7. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add groups with administrative access by following Step 5 through Step 7.
8. Click **Apply**.

To remove a **Kerberos** Administrator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. Click the check box beside the **Group Name** in the dynamic list that you want to remove from HP SMH.
5. Click **Remove**.
6. Click **Apply**.

Kerberos Operator

To add a **Kerberos** Operator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.

3. Click the **Kerberos Authorization** link.
4. In the **Kerberos Configuration** area, select the box beside **Enable Kerberos Support**.
5. In the **Group Name** textbox, enter a name in the *group@REALM* format or *REALM\groupname*.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
6. Click the **Operator** radio button beside **Type**.
7. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add groups with operator access by following steps 5 through 7.
8. Click **Apply**.

To remove a **Kerberos** Operator:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. Select the check box beside the **Group Name** in the dynamic list that you want to remove from HP SMH.
5. Click **Remove**.
6. Click **Apply**.

Kerberos User

To add a **Kerberos** User:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. In the **Kerberos Configuration** area, select the box beside **Enable Kerberos Support**.
5. In the **Group Name** textbox, enter a name in the *group@REALM* format or *REALM\groupname*.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
6. Click the **User** radio button beside **Type**.
7. Click **Add**. The values entered are added as a new line in the list table.

   You may continue to add groups with user access by following steps 5 through 7.
8. Click **Apply**.

To remove a **Kerberos** User:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Kerberos Authorization** link.
4. Select the check box beside the **Group Name** in the dynamic list that you want to remove from HP SMH.
5. Click **Remove**.
6. Click **Apply**.

User Groups category

HP SMH uses operating system accounts for authentication and enables you to manage the level of access of operating system accounts at an operating system account group level.

The users in the operating system group **Administrators** for Windows, or the operating system group **root** (which in turn contains the user root by default) for Linux, can define operating system groups that correspond to HP SMH access levels of **Administrator**, **Operator**, or **User**. After operating system groups are added, the operating system administrator can add operating system users into

these operating system groups. The Administrator is unable to add groups in SMH if one of the added group is deleted from the OS. However, the Administrator can add OS groups in SMH after re-starting the SMH service.

Each HP SMH access level can be assigned up to five operating system groups. The HP SMH installation enables you to assign the operating system groups to HP SMH. HP SMH will not allow adding an operating system group if the specified operating system group is not defined in the operating system.

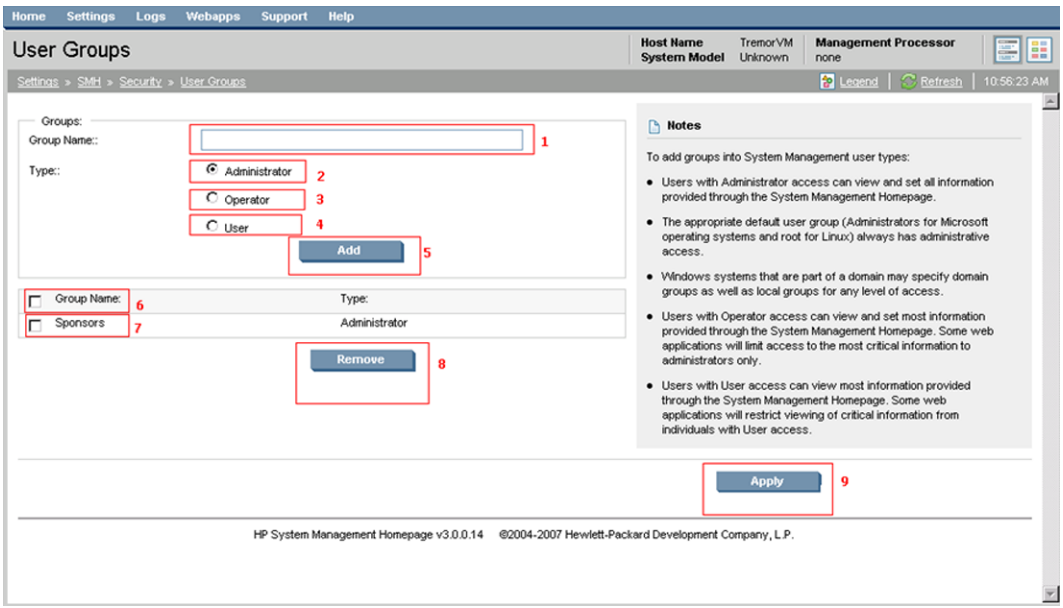
The accounts used for HP SMH do not need to have elevated access on the host operating system. Any administrative HP SMH user can specify operating system user groups to each access level of HP SMH. As a result, all accounts in each operating system user group have the access to HP SMH specified in the **User Groups** window.

NOTE: All user groups must exist in the HP System Management Homepage host system.

The Windows administrators group and the Linux root group have administrative access to the HP SMH.

For example, the HP SMH Administrator access level could be assigned the user-created operating system groups Admin1, Admin2, and Admin3. Any user that is a member of the operating system user groups (Admin1, Admin2, or Admin3) is given administrative rights on HP SMH whether the accounts have elevated access on the host operating system.

The **User Groups** page enables you to add user groups to HP SMH. The following levels of user group authorizations are available:


Home
Settings
Logs
Webapps
Support
Help
User Groups
Host Name
System Model
TremorVM
Unknown
Management Processor
none
Settings » SMH » Security » User Groups
Legend
Refresh
10:56:23 AM
Groups:
Group Name::
Type::
Administrator
Operator
User
Add
Group Name:
Sponsors
Type:
Administrator
Remove
Notes
To add groups into System Management user types:
Users with Administrator access can view and set all information provided through the System Management Homepage.
The appropriate default user group (Administrators for Microsoft operating systems and root for Linux) always has administrative access.
Windows systems that are part of a domain may specify domain groups as well as local groups for any level of access.
Users with Operator access can view and set most information provided through the System Management Homepage. Some web applications will limit access to the most critical information to administrators only.
Users with User access can view most information provided through the System Management Homepage. Some web applications will restrict viewing of critical information from individuals with User access.
Apply
1
2
3
4
5
6
7
8
9
HP System Management Homepage v3.0.0.14 ©2004-2007 Hewlett-Packard Development Company, L.P.

1 **Group Name**

All user groups must exist in the HP System Management Homepage host system.

Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.

2 **Administrator**

4 **User**

Users with **User** access can view most information provided through HP SMH. Some web applications restrict viewing of critical information from individuals with **User** access.

5 **Add**

Adds the name, level of access, and creates a new register in the list.

7 **Register**

Select respective register

8 **Remove**

Removes the selected register from the list.

9 **Apply**

Records the registers in to the .XML configuration file.

Users with **Administrator** access can view all information provided through HP SMH. The default user group, **Administrators** for Windows operating systems and **root** for Linux, always has administrative access.

3 **Operator**

Users with **Operator** access can view and set most information provided through HP SMH. Some web applications limit access to the most critical information to administrators only.

6 **Group Name Enable All**

Checks all checkboxes in the listings.

Administrator Group

To add an Administrator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. In the **Groups** area, enter a group name in the **Group Name** textbox.

   All user groups must exist in the HP System Management Homepage host system.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
5. Click the **Administrator** radio button beside **Type**.
6. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add up to five **Administrator groups** by following steps 4 through 6.
7. Select the check box beside the **Group Names** in the dynamic list you want to add to SMH.
8. Click **Apply**.

To remove an Administrator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. Select the check box beside the **Group Names** in the dynamic list that you want to remove from SMH.
5. Click **Apply**.

Operator Group

To add an Operator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. In the **Groups** area, enter a group name in the **Group Name** textbox.

   All user groups must exist in the HP System Management Homepage host system.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.

5. Click the **Operator** radio button beside **Type**.
6. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add up to five **Operator groups** by following steps 4 through 6.
7. Select the check box beside the **Group Names** in the dynamic list you want to add to SMH.
8. Click **Apply**.

To remove an Operator Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. Select the check box beside the **Group Names** in the dynamic list that you want to remove from SMH.
5. Click **Apply**.

User Group

To add a User Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. In the **Groups** area, enter a group name in the **Group Name** textbox.

   All user groups must exist in the HP System Management Homepage host system.

   Only alphanumeric and underline values are permitted. The use of special characters such as ~ ' ! @ # $ % ^ & * ( ) + = / " : ' < > ? , | ; are not permitted.
5. Select the **User** radio button beside **Type**.
6. Click **Add**. The values entered are added as a new line in the list table.

   You can continue to add up to five **User groups** by following steps 4 through 6.
7. Select the check box beside the **Group Names** in the dynamic list you want to add to SMH.
8. Click **Apply**.

To remove a User Group:

1. Select **Settings** from the menu.
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **User Groups** link.
4. Select the check box beside the **Group Names** in the dynamic list that you want to remove from SMH.
5. Click **Apply**.

Handling (proper) of the HP SMH certificate revocation

The certificate and the key files form the communication channel between HP SIM and HP SMH.

The certificate and private key generation occurs only for the first time HP SMH is started or when pairing exists between the certificate and the key files. The certificate and the key files are shared with other HP Management software, such as HP SIM. A certificate from a certificate authority (CA), such as Verisign or Entrust can replace self-generated certificates.

The following warning is displayed on the HP SMH login screen whenever the certificate or the keys or both are modified or revoked: `The certificate and keys used by HP SMH to establish SSL (https) connections have been replaced. It might have happened because the previous version was deleted (accidentally or maliciously) or replaced by another application (HP SIM replaces the certificate and keys when installed on top of SMH). Please, verify what happened to the previous version and take the appropriate actions.`

HP SMH uses the root certificate, intermediate certificate, and the Certificate Root List (CRL) of the certificate to verify the revocation status of trusted certificate used for SSO. If the certificate is found to be revoked or an error is encountered during verification, HP SMH does not allow the user to access HP SMH through SSO and redirects the user to the login page. HP SMH displays the following warning message on the login screen when the SSL certificate is revoked: `Failed to verify CA signed certificate used by SMH. See SMH logs for more details.`

Detecting and handling memory leak at runtime (Windows only)

When loaded with Webapps, HP SMH may require large memory space. An option is realized in CLI in HP SMH (Windows only) to monitor the memory usage, and if the memory usage exceeds the user specified limit or the set default limit, HP SMH reboots (soft restart) without modifying user settings.

HP SMH reads the memory usage, every 12 hours (twice a day). If the memory usage exceeds the specified limit, HP SMH reboots. A timer thread is created and Waitable Timer Object (provided by Windows SDK) is used to set the frequency of checking the memory usage. The Timer thread is designed to check the operating system time every 1 hour.

Use the following command to set the maximum memory usage limit: `smhconfig -J < max-memory-usage >` where, smhconfig is the command to modify HP SMH settings, □—J: Option to modify max-memory-usage value, <max-memory-usage> is maximum memory usage (in MB). This field accepts only unsigned integers. The default value is 60 MB. Any value below 60 MB is not accepted.

If the memory usage exceeds the specified limit, HP SMH is restarted by running smhconfig command `smhconfig -r`, which does not disturb the existing user sessions.

Alternative Names Certificates (Windows and Linux only)

HP SMH allows the setting of multihomed or multiple names to certificates that are not generated by HP. Through this functionality, SMHs certificate can contain additional information for the machine, such as other names in the network and IPs that are available. In the same way, it is possible to create a request certified to be signed by a Certificate Authority (CA).

Two kinds of values are acceptable as alternative names:

- DNS name (for example, Linux;Linux.localdomain)
- IP Address (for example, 10.16.165.1;192.168.1.189)

Only users in the Administrator User Group and System Administrators (*root* on Linux and *Administrator* on Windows) can edit the **Alternative Names** fields through the browser.

The *multihomed* configuration is available by completing the following steps:

1. Select **Settings** from the menu
2. In the **System Management Homepage** box, click the **Security** link.
3. Click the **Local Server Certificate** link.
4. In the **Current Certificate** box, enter a value in the **Alternative Names** field.
5. Click **Create**.
6. Click **Yes** and the previous page appears with the message: `Success: Value successfully changed`.

When this happens, the new certificate with the alternative names set are negotiated with the browser.

Menus (HP-UX only)

The **Menus** category provides links to add custom menus and remove custom menus:

- Select **Settings→Menus→Add Custom Menu**.
- Select **Settings→Menus→Remove Custom Menu**.

Add Custom Menu (HP-UX only)

To add a custom menu to HP SMH (HP-UX only):

1. Select **Settings**→**Menus**→**Add Custom Menu**.
2. For **Type**, specify whether the menu is a command execution, an X application launch, or a link to another Web site or Web application.
3. For **Page**, specify the page HP SMH pages that the menu should be under.

   For example, you can specify **Home**, **Tasks**, **Settings**, **Tools**, or **Logs**.
4. For **Category**, specify a category (box) for the menu to be placed under.

   You can provide the name of an existing category or enter a new category, which is created.
5. For **Tool Name**, enter the name of the menu as you want it to appear under the Page and Category specified.
6. For **Command/URL**, enter the command line to the command or X application, or the URL to the Web page that is the target of the link.
7. For **Run as root**, select the check box on the right to specify that the command runs as the root user.

   If selected, only HP SMH users with Administrator privileges are allowed to run this menu.

Only HP SMH users with Administrator authorization can create menus and can run custom menus that are set to run as the "root" user. For HP SMH users with Operator or User authorization, the custom menus they are allowed to run are run as the user id of the user logged in.

These custom menus are stored and managed in the `/opt/hpsmh/data/htdocs/xlaunch/custom-menus.js` file, which can be manually copied from one system to other systems.

Remove custom menu (HP-UX only)

To access the Remove Custom Menu, select **Settings**→**Menus**→**Remove Custom Menu**.

7 The Tasks page

The **Tasks** page displays links to routine tasks provided by participating HP Web-enabled System Management Software.

If no tasks are provided by HP Web-enabled System Management Software, the **Tasks** page is not visible.

8 The Tools page (HP-UX only)

The **Tools** page displays links to system management tools provided by participating HP Web-enabled System Management Software. For HP-UX, the **Tools** page provides an entry point into management tools that are analogous to the System Administration Manager (SAM) main page, also known as the SAM Functional Area Launcher (or FAL). For HP-UX this also includes categories and menus for several X-based management applications. Some links that you may see on the **Tools** page follow:

- Accounts for Users and Groups
- Auditing and Security Attributes Configuration
- Authenticated Commands (PAM)
- Disks and File Systems
- Distributed Systems Administration Utilities (DSAU)
- Evweb
- Integrated Agents and Other Agents
- IPMI Event Viewer
- Kernel Configuration
- Networking and Communications
- nPartition Management
- Peripheral Devices
- Printer Management
- Resource Management
- Resource Monitors
- Serviceguard
- Software Management
- Time

Each of these functional areas has its own associated online help.

If no tools are provided by the HP Web-enabled System Management Software, the **Tools** page is not visible.

9 The Logs page

At a minimum, the **Logs** page provides the following log categories:

- System Management Homepage Log
- Httpd Error Log (Windows and Linux)

Logs contained in the installed HP Web-enabled System Management Software appear on this page. For example, if the HP Version Control Agent is installed, a link to the Version Control Agent log appears on the **Logs** page. As another example, if the Distributed Systems Administration Utilities (DSAU) is installed, a link to the System Log Viewer appears on the **Logs** page. Each log file is divided into pages that display a total of 40 log entries to a page.

System Management Homepage Log

The **System Management Homepage Log** contains HP System Management Homepage (HP SMH) configuration changes as well as successful and failed sign-in attempts. It is helpful when troubleshooting sign-in or access issues when signing in directly to HP SMH, or from the HP Systems Insight Manager (HP SIM).

You must have administrative access to HP SMH to access the **System Management Homepage Log**.

To access the HP SMH Log, select **Logs** from the menu and click the **System Management Homepage Log** link in the **System Management Homepage** box.

SAM Log

The **SAM Log** link provides access to the **SAM Log Viewer**. The **SAM Log Viewer** provides a Web interface into the HP-UX System Administration Manager (SAM) log file. This log file is used by existing SAM applications and the new Web-based management applications.

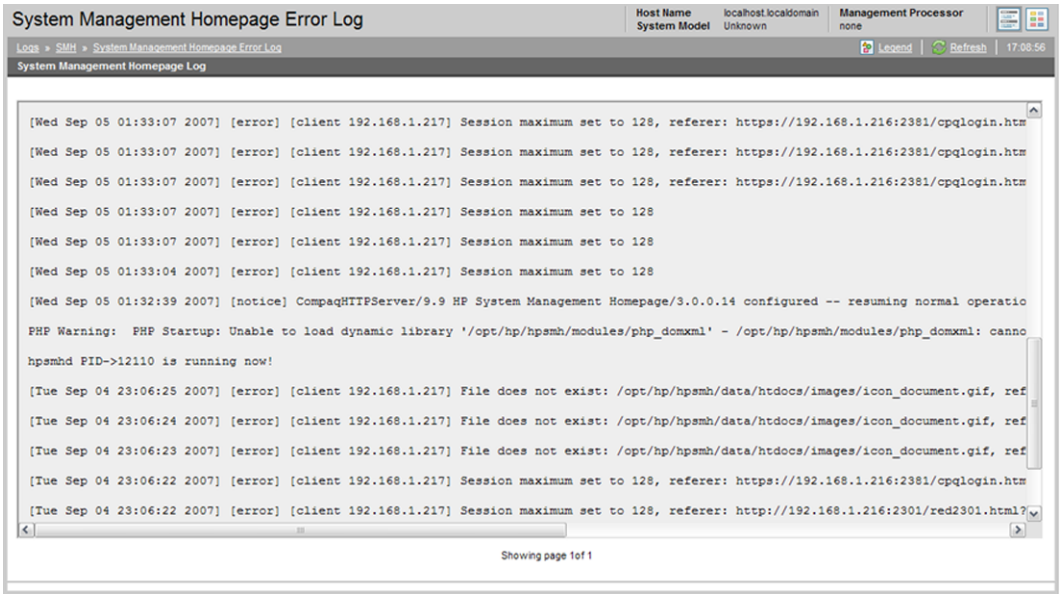
The **SAM Log** is available on HP-UX only.

To access the SAM Log, select **Logs** from the menu and click the **SAM Log** link in the **System Management Homepage** box.

To filter messages from the SAM Log, select the criteria to filter by, and then click **OK**. The messages appear at the bottom of the screen.

Httpd Error Log

The **Httpd Error Log** contains error information generated by HP SMH modules, Kerberos misconfiguration errors, and CGI execution errors (httpd). It is the first place to look when a problem occurs with starting the server or with server operation because the log often contains details of what went wrong and how to fix the problem.


System Management Homepage Error Log
Host Name localhost.localdomain
System Model Unknown
Management Processor none
Logs » SMH » System Management Homepage Error Log
Legend
Refresh
17:08:56
System Management Homepage Log
[Wed Sep 05 01:33:07 2007] [error] [client 192.168.1.217] Session maximum set to 128, referer: https://192.168.1.216:2381/cpqlogin.htm
[Wed Sep 05 01:33:07 2007] [error] [client 192.168.1.217] Session maximum set to 128, referer: https://192.168.1.216:2381/cpqlogin.htm
[Wed Sep 05 01:33:07 2007] [error] [client 192.168.1.217] Session maximum set to 128, referer: https://192.168.1.216:2381/cpqlogin.htm
[Wed Sep 05 01:33:07 2007] [error] [client 192.168.1.217] Session maximum set to 128
[Wed Sep 05 01:33:07 2007] [error] [client 192.168.1.217] Session maximum set to 128
[Wed Sep 05 01:33:04 2007] [error] [client 192.168.1.217] Session maximum set to 128
[Wed Sep 05 01:32:39 2007] [notice] CompaqHTTPServer/9.9 HP System Management Homepage/3.0.0.14 configured -- resuming normal operatio
PHP Warning: PHP Startup: Unable to load dynamic library '/opt/hp/hpsmh/modules/php_domxml' - /opt/hp/hpsmh/modules/php_domxml: canno
hpsmhd PID->12110 is running now!
[Tue Sep 04 23:06:25 2007] [error] [client 192.168.1.217] File does not exist: /opt/hp/hpsmh/data/htdocs/images/icon_document.gif, ref
[Tue Sep 04 23:06:24 2007] [error] [client 192.168.1.217] File does not exist: /opt/hp/hpsmh/data/htdocs/images/icon_document.gif, ref
[Tue Sep 04 23:06:23 2007] [error] [client 192.168.1.217] File does not exist: /opt/hp/hpsmh/data/htdocs/images/icon_document.gif, ref
[Tue Sep 04 23:06:22 2007] [error] [client 192.168.1.217] Session maximum set to 128, referer: https://192.168.1.216:2381/cpqlogin.htm
[Tue Sep 04 23:06:22 2007] [error] [client 192.168.1.217] Session maximum set to 128, referer: http://192.168.1.216:2301/red2301.html?
Showing page 1of 1

The **Httpd Error Log** is available on HP-UX directly but is visible in Windows and Linux by adding the *httpd-error-log* tag in the `smhpd.xml` file.

You must have administrative access to HP SMH to access the **Httpd Error Log**.

For HP SMH 3.x and later, it is possible to display the httpd error log in the HP SMH user interface using the `smhconfig` tool as follows:

To enable displaying the error log:

```
smhconfig -p or --httpd-error-log True
```

To disable displaying the error log:

```
smhconfig -p or --httpd-error-log False
```

HP SMH must be restarted to apply the new configuration.

To restart the HP SMH service:

```
smhconfig -r
```

To access the **Httpd Error Log**:

Select **Logs** from the menu and click the **Httpd Error Log** link in the **System Management Homepage** box.

Supported languages

HP SMH is only localized to English and Japanese, that is, by default the HP SMH Logs and UI supports English and Japanese. Also, HP SMH supports webapps and localizes their help to English, French, Italian, German, Spanish, Korean, Simplified Chinese, Traditional Chinese, and Japanese languages. To display the messages properly, the necessary fonts must be installed on the system. For example, on a non-Japanese version of Windows, the user must install Japanese fonts to read the log in that language.

The following table contains the locale names for the languages that HP SMH supports:

Table 5 Locale names of supported languages

Language	Linux locale name	Windows locale name
English	en_US.UTF-8	english
Japanese	ja_JP.UTF-8	japanese
German	de_DE.UTF-8	german

Table 5 Locale names of supported languages *(continued)*

Language	Linux locale name	Windows locale name
Spanish	es_ES.UTF-8	spanish
French	fr_FR.UTF-8	french
Italian	it_IT.UTF-8	italian
Korean	ko_KR.UTF-8	korean
Simplified Chinese	zh_CN.UTF-8	chinese-simplified
Traditional Chinese	zh_TW.UTF-8	chinese-traditional

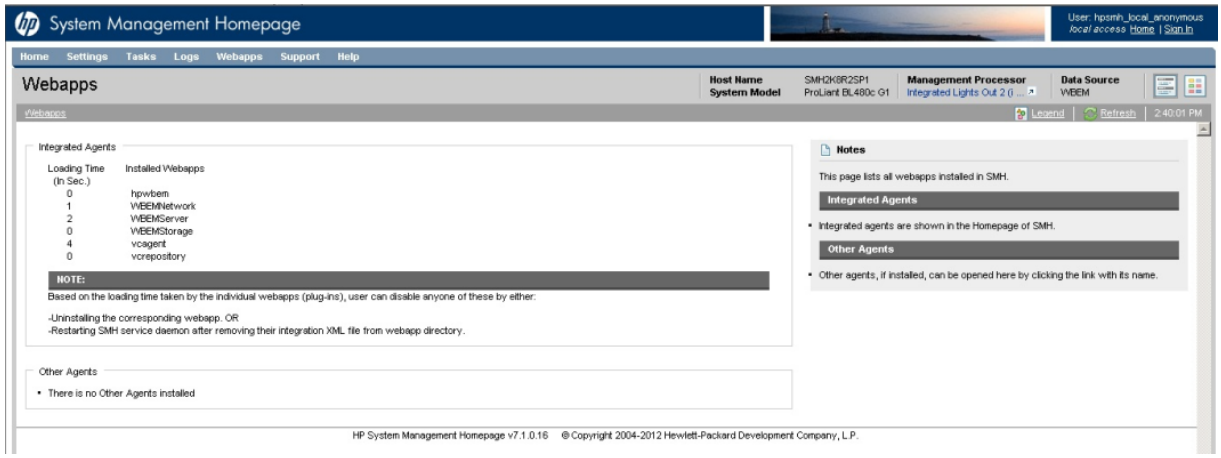
The following table contains the suffixes of the `log_messages.php` pages according to each supported language:

Table 6 Suffixes of supported languages

Language	Suffix
English	en
Japanese	ja
German	de
Spanish	es
French	fr
Italian	it
Korean	ko
Simplified Chinese	zh
Traditional Chinese	zh

10 The Installed Webapps page (Windows and Linux only)

The **Installed Webapps** page contains a list of installed Webapps in the HP System Management Homepage (HP SMH). It contains links to the following HP Web-enabled System Management Software:


System Management Homepage
Home
Settings
Tasks
Logs
Webapps
Support
Help
Webapps
Integrated Agents
Loading Time (In Sec.)
Installed Webapps
0 hpwbem
1 WBEMNetwork
2 WBEMServer
0 WBEMStorage
4 vcagent
0 vcrepository
NOTE:
Based on the loading time taken by the individual webapps (plug-ins), user can disable anyone of these by either:
-Uninstalling the corresponding webapp. OR
-Restarting SMH service daemon after removing their integration XML file from webapp directory.
Other Agents
There is no Other Agents installed
Notes
This page lists all webapps installed in SMH.
Integrated Agents
Integrated agents are shown in the Homepage of SMH.
Other Agents
Other agents, if installed, can be opened here by clicking the link with its name.
HP System Management Homepage v7.1.0.16 © Copyright 2004-2012 Hewlett-Packard Development Company, L.P.

Integrated Agents

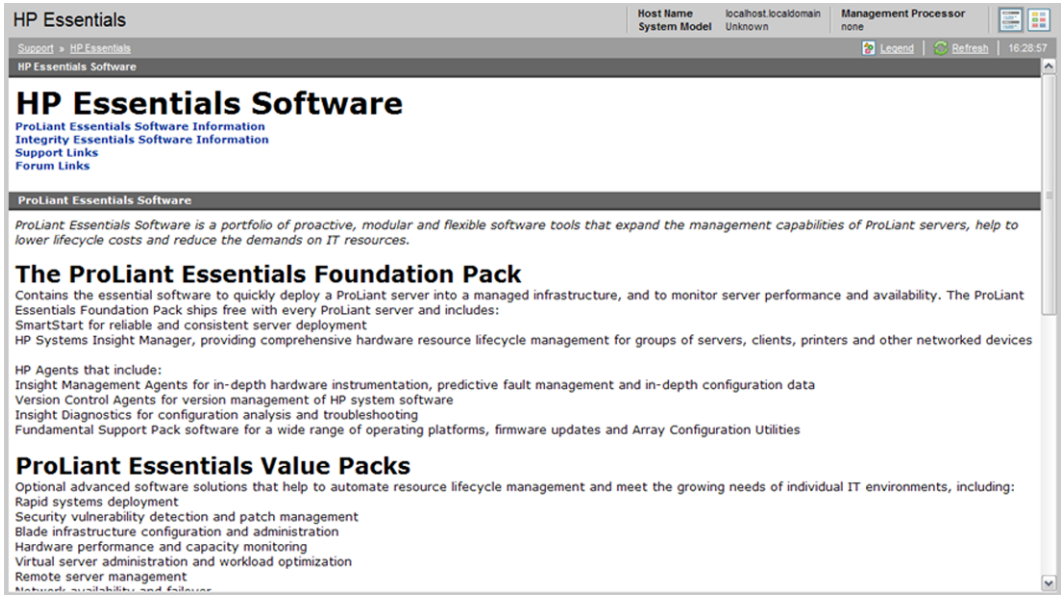
Lists Webapps names. Participants are agents that contribute information contained in HP SMH. If no HP Web-enabled System Management Software is installed that provides this information, an informative message appears. Information about the **Loading time (in sec)** for each of the **Installed Webapps** is provided in the Integrated Agents field.

Other Agents

Lists the visible HP Web-enabled System Management Software. The name of the HP Web-enabled System Management Software provides a link so you can access the agents if they provide a user interface. When you click the link, the webapp is opened in a new browser window. If no HP Web-enabled System Management Software is installed that provides this information, an informative message appears.

11 The Support page

The **Support page** provides information about HP Essentials Software and instructions on how to obtain guidance from HP Support and official forums. This page also provides the following links for help outside the HP System Management Homepage server domain.


HP Essentials
Host Name
System Model
localhost.localdomain
Unknown
Management Processor
none
Support » HP Essentials
Legend
Refresh
16:28:57
HP Essentials Software
HP Essentials Software
ProLiant Essentials Software Information
Integrity Essentials Software Information
Support Links
Forum Links
ProLiant Essentials Software
ProLiant Essentials Software is a portfolio of proactive, modular and flexible software tools that expand the management capabilities of ProLiant servers, help to lower lifecycle costs and reduce the demands on IT resources.
The ProLiant Essentials Foundation Pack
Contains the essential software to quickly deploy a ProLiant server into a managed infrastructure, and to monitor server performance and availability. The ProLiant Essentials Foundation Pack ships free with every ProLiant server and includes:
SmartStart for reliable and consistent server deployment
HP Systems Insight Manager, providing comprehensive hardware resource lifecycle management for groups of servers, clients, printers and other networked devices
HP Agents that include:
Insight Management Agents for in-depth hardware instrumentation, predictive fault management and in-depth configuration data
Version Control Agents for version management of HP system software
Insight Diagnostics for configuration analysis and troubleshooting
Fundamental Support Pack software for a wide range of operating platforms, firmware updates and Array Configuration Utilities
ProLiant Essentials Value Packs
Optional advanced software solutions that help to automate resource lifecycle management and meet the growing needs of individual IT environments, including:
Rapid systems deployment
Security vulnerability detection and patch management
Blade infrastructure configuration and administration
Hardware performance and capacity monitoring
Virtual server administration and workload optimization
Remote server management

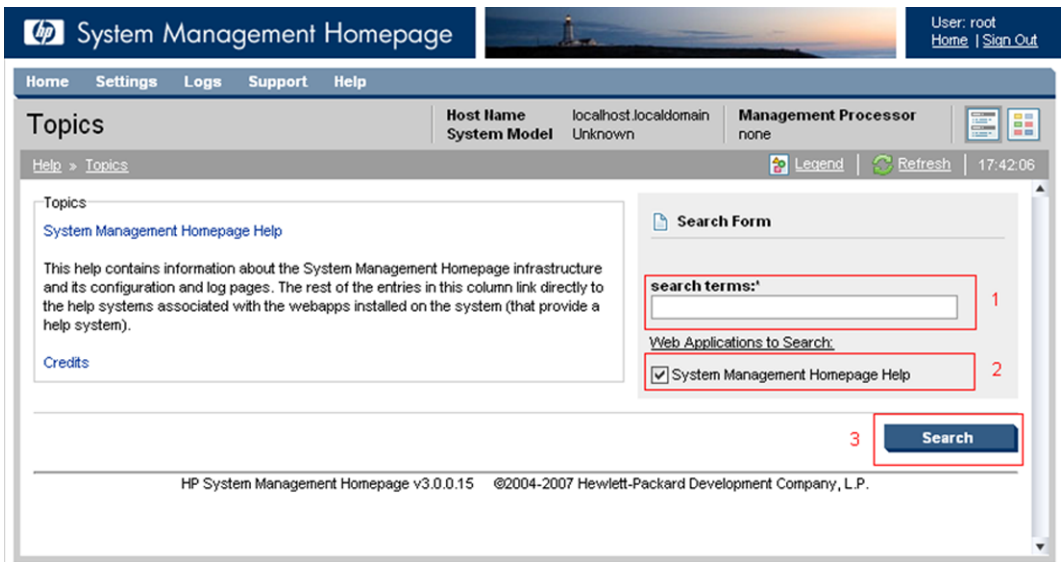
- Insight Essentials Software Information
- Integrity Essentials Software Information
- Support Links

  In HP-UX, the support link opens the HP Support Center (HPSC) home page.
- Forum Links

  In HP-UX, the forum link opens the HP Support Center (HPSC) Forums page.

The Help page

The **Help page** provides help for the HP System Management Homepage (HP SMH) and its webapps.



1 **Search terms**

Enables you to enter search criteria.

2 **Webapp to search**

3 **Search**

Validates search field and chosen webapp.

The **Help page** provides links for the following:

- **System Management Homepage Help**

  Contains information about the HP SMH infrastructure and its configuration and log pages. The remaining entries link to help systems associated with the webapps installed on the system (those that provide a help system).

- **Credits**

  Displays information regarding open source licensing and credits.

To access HP SMH help, complete the following steps:

1. Click **Help**.
2. Click the **System Management Homepage Help** link.

To access **Credits**, complete the following steps:

1. Click **Help**.
2. Click the **Credits** link.

Search form

The **Search Form** section provides a field for you to input a search term to search the HP SMH help.

To execute a search, complete the following steps:

1. In the **search terms** textbox in the **Search Form** section, enter a search term.
2. Click **Search**.

   If the search criteria is valid, a list of all documents matching the query appears.

Credits

The **Credits** link displays information regarding open source licensing and credits.

To access Credits, select **Help** and click the **Credits** link.

12 Command Line Interface configuration

The Command Line Interface (CLI) provides users with administrative rights access to set these values through the command line. You can use the CLI to modify configuration options, including the required security checks that allow the configuration options to be changed.

NOTE: –kerberos, --user-kerberos, --operator-kerberos, --admin-kerberos, –max-threads and --win32-disable-acceptex options are only available on Windows operating systems.

NOTE: Long options, starting with "--", have an optional symbol "=" before the argument.

Some CLI options require special arguments listed as words in capital letters in the option summary of the command. Descriptions of the format of these arguments are in the following table:

Table 7 CLI arguments

Argument type	Description
DIR	A path to a directory where the HP SMH service has write access.
FILE	A path to a file.
GROUPLIST	A list of group names separated by semicolons.
IPBINDLIST	A list of IPv6 addresses and/or IPv4 address/netmask pairs separated by semicolons.
IPLIST	A list of IP addresses separated by semicolons.
NUM	A numeric value with a range that depends on the option being set.
NAMELIST	A list of host names and IP addresses separated by semicolons.
XENAMELIST	A list of trusted server host names.

Anonymous Access

Anonymous access allows anonymous users to access unsecured pages, including local anonymous access. The following command enables or disables the anonymous access setting:

```
smhconfig -a|--anonymous-access[=] True | False
```

Display Current Settings (Windows and Linux only)

The `smhconfig` CLI command is used to modify the various HP SMH settings. However, the only way to view the current settings is through the browser. A new option is introduced in smhconfig as“—V ” or “—display -current-settings” which displays the current settings of SMH.

To view the current HP SMH settings, run the following command:

```
smhconfig -V|--display-current-settings
```

NOTE: `smhconfig -V|--display-current-settings` command displays value as "NULL" if no HP SMH settings are set.

Local Access

The local access command sets the local access privilege to anonymous or administrator, applying the specified access to the local system. If local access is selected, a user with access to the local console is granted anonymous or administrator access without being challenged for a username and password.

The following command enables or disables local access:

```
smhconfig -L|--localaccess-enabled[=] True | False
```

The following command configures the local user privileges:

```
smhconfig -l|--localaccess-type[=] administrator | anonymous
```

IP Restricted Logins

IP addresses can be explicitly permitted or restricted based on user type. If there are IP addresses in the permitted list, only those IP addresses are allowed login access. If there are no IP addresses in the permitted list, login access is granted to any IP address not in the restricted list.

The following command enables or disables IP restricted login:

```
smhconfig -P|--ip-restricted-logins[=] True | False
```

IP Address Inclusion

Perform the IP address permitted command as follows:

```
smhconfig -i|--ip-restricted-include[=] IPLIST
```

The following is an example of how *IPLIST* is formatted:

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

IP Address Exclusion

Perform the IP address restricted command as follows:

```
smhconfig -e|--ip-restricted-exclude[=] IPLIST
```

The following is an example of how *IPLIST* is formatted:

122.23.44.1-122.23.44.255;172.84.100.35;172.168.10.5;168.172.10.1-168.172.10.128

NOTE: For systems running on Windows and Linux, IPv4 and IPv6 address ranges are supported. For systems running on HP-UX operation system, currently, IPv4 address ranges are supported.

IP Binding

IP binding provides HP SMH the ability to listen only to the addresses configured in the IP binding list. If IP binding is enabled and the IP binding list is empty, HP SMH will only be accessible locally.

Perform the IP binding command as follows:

```
smhconfig -g|--ip-binding[=] True | False
```

IP binding list

Use the following command to configure the IP binding list to be used when IP binding is enabled.

```
smhconfig -I|--ip-binding-list[=] IPBINDLIST
```

IPBINDLIST must be a list of semicolon-separated IP addresses and/or IP address/netmask pairs.

The following is an example of how *IPBINDLIST* is formatted:

172.24.31.10/255.255.255.0;128.88.236.189/255.255.255.0;172.25.86.69/255.255.0.0

Trust Modes

The HP SMH trusts HP SIM or HP Insight Manager 7 (IM 7) secure task execution requests and single sign on requests with various levels of security, ranging from trust all to only trust HP SIM or HP Insight Manager 7 with trusted certificates:

- **Trust All**

  This command sets up the http server to accept all secure task execution requests and single sign on requests from any HP SIM or HP Insight Manager 7 7 server:

  ```
  smhconfig -t|--trustmode[=] TrustByAll
  ```

- **Trust By Name**

  This command sets up the HP SMH to only accept secure task execution requests and single sign on requests from the listed HP SIM or HP Insight Manager 7 7 servers:

  ```
  smhconfig -t|--trust-mode[=] TrustByName
  ```

  To configure the trusted servers name list for the TrustByName trust mode, use the following command:

  ```
  smhconfig -X|--xenamelist[=] XENAMELIST
  ```

  XENAMELIST is a list of the HP SIM or HP Insight Manager 7 7 servers that trust, using a comma or semicolon as a delimiter. The following is an example of the name list format:

  ```
  server1,server2.domain1;server3,server4.domain2
  ```

- **Trusted Certificates**

  This command establishes the trust relationship between HP SIM or HP Insight Manager 7 7 and the HP SMH using the certificate. The trust mode is set to TrustByCert using the following command:

  ```
  smhconfig -t|--trustmode[=] TrustByCert
  ```

  A trusted certificate is added to the trusted certificate list using the following command:

  ```
  smhconfig -C|--trust-certificate[=] FILE
  ```

  FILE is the name of the file containing the base 64 encoded certificate to be added to the trusted certificate list.

Restart service

Restart the HP SMH on completion of applying the new configuration settings.

```
smhconfig -r|--restart
```

Reject Program Admin Login (Windows and Linux only)

Reject or accept and Web-enabled System Management Software or HP VCA login request.

```
smhconfig -j|--reject-prog-admin-login[=] true|false
```

Win32DisableAcceptEX

AcceptEX() is a Microsoft WinSock v2 API that provides performance improvements over the use of the BSD style accept() API in specific circumstances. Some popular Windows products, typically virus scanning or virtual private network packages, have bugs that interfere with the operation of AcceptEx(). If you encounter an error condition like:

```
[error] (730038) An operation was attempted on something that is not a
socket:: winnt_accept: AcceptEx failed. Attempting to recover.
```

Use the following directive to disable the use of AcceptEx():

```
smhconfig -w|--win32-disable-acceptex[=] True | False
```

NOTE: Win32DisableAcceptEX is only available on Windows operating systems.

Enable/disable SSL v2

By default the HP SMH has SSL v2 disabled. Use the following switch to re-enable SSL v2:

```
smhconfig -s|--disable-sslv2[=] True | False
```

where *value False* enables SSL v2 and *value True* disables SSL v2

Execute the following command to restart the HP SMH service `smhconfig -r`.

Log Rotations (Windows and Linux only)

Log files can become large and unmanageable. The following switch enables log files to rotate automatically when they reach 5M (default size). Either the log file is overwritten on the next rotation when the option is off or a new file is created and the previous file is marked as old when the option is on.

```
smhconfig -A|--rotate-logs[=] 0 | 1 | 2
```

Where: 0= off, 1 or 2= on.

Rotate Log Size (Windows and Linux only)

Log files over a period of time can become large and unmanageable. The following command switch allows the user to set the size of the log files.

```
smhconfig -z|--rotate-log-size[=] size
```

Where size is a value in the range of 1-9MB.

Maximum Number of Threads Allowed

The **Maximum Number of Threads Allowed** value allows the user to increase or reduce the maximum number of threads HP SMH creates to handle page requests. The default is 64 for Windows.

NOTE: Maximum Number of Threads Allowed is only available on Windows operating systems.

```
smhconfig -M|--max-threads[=] max-number-of-threads
```

Where *max-number-of-threads* is a number in the range of 64-512.

Maximum Number of Threads Allowed is only available on Windows.

Maximum Number of Sessions (Windows and Linux only)

By default, HP SMH supports 128 user sessions. This number can be lowered to 32 or raised to 500 using the `session-maximum` setting.

```
smhconfig -S|--session-maximum[=] maximum-number-of-sessions
smhconfig -S|--session-maximum[=] 32-500
```

Session Timeout

For systems running on Windows and Linux, the default session timer is set to 15 minutes. The session timeout can be set as low as 1 minute or as high as 60 minutes.

For systems running on HP-UX, the default session timer is set to 15 minutes. The session timeout can be set as low as 6 minute or as high as 120 minutes.

```
smhconfig -U|--session-timeout[=] session-timeout-in-minutes
```

UI Timeout

The UI timeout value represents the maximum amount of time in seconds that the HP SMH user interface (UI) waits for data requested from webapps.

The UI timeout can be set in the range of 10 seconds to 3600 seconds.

Use the following command used to set the UI Timeout in seconds:

```
smhconfig - B|--ui-timeout[=] NUM
```

where, NUM is the value (in seconds) between the range 10 seconds to 3600 seconds.

The default UI Timeout value set is 120 seconds.

Log level

By default, the logging level of HP SMH error messages is set to `error`. When a log level is set, all events that are the same or superior to the configured log level are written to the log file. The log level option only affects the `error_log` file located under *`SystemDrive:`*`\hp\hpsmh\logs` in Windows and under `/var/spool/opt/hp/hpsmh/logs` in Linux.

The following values are available, in order of decreasing significance:

Table 8 Log level

Value	Description
emerg	Emergencies - system is unusable
alert	Action must be taken immediately
crit	Critical conditions
error	Error conditions
warn	Warning conditions
notice	Normal but significant condition
info	Informational
debug	Debug-level messages

```
smhconfig -v|--log-level[=] logging-level
```

NOTE: Log level only affects new messages written in the HTTP error log. You must perform a soft restart of the system.

Port 2301

Port 2301 determines whether HP SMH listens on port 2301. If the value is set to **True**, HP SMH listens on port 2301. If the value is set to **False**, HP SMH does not listen on port 2301.

The default is set to True.

```
smhconfig -T|--port2301[=] True | False
```

Multihomed certificate alternative names list

You can set the **name** for the certificate through the multihomed option.

It is important to restart the hpsmhd service when running smhconfig with multihomed values using a single command on the console (`--restart` option).

```
smhconfig -u|--multihomed[=] NAMELIST
```

```
smhconfig -u|--multihomed[=] NAMELIST --restart
```

`NAMELIST` must be a semicolon-separated list of IP addresses and hostnames.

Custom UI

Enabling custom UI enables you to customize the sign-in and header images as well as adding a small text in the sign-in page. See the HP SMH `README.txt` in the `hpsmh/data/htdocs/custom_ui` directory in the HP SMH install path.

```
smhconfig -c|--custom-ui[=] True | False
```

Log-based directory

To define a particular directory location (path) to the `smh error_log` and `access_log`, use the following command:

```
smhconfig -O|--log-base-dir[=] DIR
```

where, DIR is the directory location (path) of the directory where the log is to be saved.

Configurable logging

To configure the logs in HP SMH, execute the following command:

`smhconfig -q |--config-level[=] Informational | Minor | Warning | Major | Critical` where, Informational, Minor, Warning, Major, and Critical are the logging levels in HP SMH.

Execute the following command to restart the HP SMH service `smhconfig -r`.

Any logs of severity greater than or equal to the configuration level set is logged in the `smh_enc.log` file.

Autostart mode

Autostart mode is a feature in HP SMH which, if enabled, stops the Apache server after a user-specfied timeout (server timeout) period to optimize the system resources. Beyond the server timeout period set, HP SMH cannot be accessed through port 2381 until it is accessed via port 2301 and thus auto starting HP SMH on port 2381.

Autostart mode is supported for systems running on Linux operating systems. By default, in HP SMH 6.2 first installation, Autostart mode is disabled on the HP SMH systems. It can be enabled either from the GUI or through the Command Line Interface.

To configure autostart mode start up from the Command Line Interface, execute the following command:

```
smhconfig -D|--autostart TRUE|FALSE
```

where, selecting TRUE enables the autostart mode and FALSE disables the autostart mode.

When Autostart mode is enabled, you can set the timeout in minutes for the server timeout value between 1 and 60 minutes (default value is 30 minutes)

To set the server timeout in minutes, execute the following command: `smhconfig -F|--timeoutsmh(1-60)`

where, (1-60) corresponds to the time in minutes for the server timeout.

Restart the HP SMH application for the Apache server to use the newly-configured values.

NOTE: Enabling the Autostart mode enables port 2301.

Httpd Error log

The **httpd error log** option enables you to determine if it is possible to view the httpd `error_log` log file through the user interface.

```
smhconfig -p|--httpd-error-log[=] True | False
```

Icon view

Icon view allows you to set the default view mode to show icons (True) like a desktop File Manager appearance or to show the traditional list (False) that displays items in boxes.

```
smhconfig -n|--iconview[=] True | False
```

Box Order

Box order defines the ordering method used to display the boxes. You can choose **name**, which places the boxes in alphabetical order, or you can choose **status**, which displays the boxes from the worst status (critical) to the best status (normal).

```
smhconfig -x|--box-order[=] Name | Status
```

Box Item Order

Box item order defines the ordering method used to display the items inside boxes. You can choose **name**, which places, boxes in alphabetical order, or you can choose **status**, which displays boxes from the worst status (critical) to the best status (normal).

```
smhconfig -b|--box-item-order[=] Name | Status
```

Kerberos Authentication

To enable or disable Kerberos authentication support, use the following command:

```
smhconfig -k|--Kerberos[=] True | False
```

Administrator Kerberos users

To configure Kerberos groups of users from a Kerberos domain with administrator privileges, use the following command:

```
smhconfig - m|--admin-kerberos[=] GROUPLIST
```

Note: `GROUPLIST` is a single Kerberos group or a list of Kerberos group names separated by semicolons.

NOTE: –admin-kerberos is only available on Windows operating systems.

Operator Kerberos users

To configure Kerberos groups of users from a Kerberos domain with operator privileges, use the following command:

```
smhconfig - R|--operator-kerberos[=] GROUPLIST
```

Note: `GROUPLIST` is a single Kerberos group or a list of Kerberos group names separated by semicolons.

NOTE: –operator-kerberos is only available on Windows operating systems.

User Kerberos users

To configure Kerberos groups of users from a Kerberos domain with user privileges, use the following command:

```
smhconfig - K|--user-kerberos[=] GROUPLIST
```

Note: `GROUPLIST` is a single Kerberos group or a list of Kerberos group names separated by semicolons.

NOTE: –user-kerberos is only available on Windows operating systems.

User Groups

User Groups are a set of policies to access and modify HP SMH functionalities. Only valid existing operating system groups can be added to the group list.

To add groups into HP SMH user types, complete the following:

Administrators

Users with Administrator access can view and set all information provided throughout the HP SMH.

The default user group (*Administrators* for Microsoft operating systems and *root* for Linux) always has administrative access.

Windows systems that are part of a domain can specify domain groups and local groups for any level of access.

```
smhconfig -d|--admin-group[=] [ groupList ]
```

Operators

Users with Operator access can view and set most information provided through the HP SMH. Some web applications limits access to the most critical information to administrators only.

```
smhconfig -E|--operator-group[=] [ groupList ]
```

Users

Users with User access can view most information provided through the HP SMH. Some web applications restricts viewing of critical information from individuals with User access.

```
smhconfig -G|--user-group[=] [ GROUPLIST ]
```

Where *groupList* is a single operating system group or a list of operating system group names separated by semicolons.

Help message

To display a help message on the screen, use the following command:

```
smhconfig -h|--help
```

File-based Command Line Interface

The Command Line Interface (CLI) option enables a file with configuration parameters to be passed on the command line. The CLI parses the file and processes the arguments. The command to use a file for the input to the CLI is:

```
smhconfig -f|--configfile FILE
```

Command Line Interface File Structure

The CLI file structure format includes the # character for comments, a bracketed key word indicating the parameter to be set, and the parameter value. An example of the CLI file structure format is as follows:

Characters placed after the # on a given line are not parsed.

An example of a configuration file for smhconfig is as follows:

```
# SMH configuration file for smhconfig
[anonymous-access]
false
[localaccess-enabled]
true
[localaccess-type]
administrator
[user-group]
```

`users`

Command Line Log Reader

The command line log reading tool provides the users with a command line tool for reading the SMH log messages without using the UI. The command is:

`smhlogreader [options]`

where, the [options] are:

`-h|--help`, displays the help message.

`--version`, displays the HP SMH version.

`-f|--file FILE`, FILE represents a path to a file.

`--from FROM`, FROM: to display a range of messages, this option describes the ID of the first message.

`--to TO`, TO: to display a range of messages, this option describes the ID of the last message.

`-l|--lang LANG`, LANG: the language used to display the log messages.

IMPORTANT: smhlogreader CLI also allows the combined use of these options in a single command.

For example, `smhlogreader --lang LANG --from FROM --to TO --file FILE`

The different options provided by the smhlogreader CLI are:

- Help

  It allows the user to run the command to display the help message for this tool.

  The following command displays the help message for the smhlogreader CLI.

  `smhlogreader -h|--help`

- Version

  It allows the user to run the command to display the version of HP SMH.

  The following command displays the HP SMH version number.

  `smhlogreader --version`

- Language

  It allows the user to select language of choice for the messages to be displayed

  The following command allows the user to select the language of choice for the messages to be displayed.

  `smhlogreader -l|--lang en|ja`

  By default the HP SMH Logs and UI supports “en” for English and “ja” for Japanese.

  NOTE: To display the messages properly, the necessary fonts to display the messages must be installed on the system. For example, on a non-Japanese version of Windows the user needs to install Japanese fonts to read the log in that language.

- Reading Logs

  It displays a list with the most recent messages.

  The following command displays a list with the most recent messages.

  `smhlogreader`

- Range

  It allows the user to set the range of messages that smhlogreader CLI should display.

The following command displays a list of messages in the range selected by the user.

`smhlogreader --from VALUE --to VALUE`

For example, to display messages the recent five messages, the user should use the following command: `smhlogreader --from 1 --to 5`

- File-based command line log reading

  The smhlogreader CLI allows the user to use a properly-formatted log file as an input.

  The following command allows the user to use a properly-formatted log file as an input and also backs up the log files.

  `smhlogreader - f|--file FILE`

SSL Cipher Suite configuration

To configure the Cipher Suite, use the following command:

`smhconfig -Z|--ssl-cipher-suite[=] SSLCIPHERSUITE` where, SSLCIPHERSUITE is the Cipher Suite available for configuration.

NOTE: The default SSLCIPHERSUITE is `ALL:!ADH:!EXPORT56:!EXPORT40:RC4+RSA:+HIGH:+MEDIUM:SSLv2?:+EXP:-LOW:+eNULL`.

The `?` is either `+` or `-` depending on whether SSLv2 is enabled or disabled.

Restart the HP SMH application for the Apache server to use the newly configured cipher suite.

For information on the ciphers suite available for configuration and for their description and syntax, see "Ciphers used in HP SMH" (page 86).

Change locality

Use the CLI `smhconfig -N` option to modify the fields like the Country, State, and Location, that are hard coded, in a new SMH self-signed certificate which generated whenever the SMH self-signed certificate gets corrupted or deleted accidentally.

To modify these fields, run the following command: `smhconfig -N|| --certificate-locality[=] LOCALITYINFO` where, LOCALITYINFO is the locality information in Country, State, and Locality format.

Detecting and handling memory leak at runtime (Windows only)

When loaded with Webapps, HP SMH may require large memory space. An option is realized in CLI in HP SMH (Windows only) to monitor the memory usage, and if the memory usage exceeds the user specified limit or the set default limit, HP SMH is restarted (soft restart) without modifying user settings.

HP SMH reads the memory usage, every 12 hours (twice a day). If the memory usage exceeds the specified limit, HP SMH is restarted. A timer thread is created and Waitable Timer Object (provided by Windows SDK) is used to set the frequency of checking the memory usage. The Timer thread is designed to check the operating system time every 1 hour.

Use the following command to set the **max-memory-usage** tag: `smhconfig -J < max-memory-usage >` where, smhconfig is the command to modify HP SMH settings, —J is the option to modify max-memory-usage value, and <max-memory-usage> is the maximum memory usage set by the user (in MB). This field accepts only unsigned integers. The default value is 60 MB. Any value below 60 MB is not accepted.

If the memory usage exceeds the specified limit, HP SMH is restarted by running smhconfig command `smhconfig -r`, which does not disturb the existing user sessions.

13 Troubleshooting topics

NOTE: If noted, a topic might only apply to the HP-UX, Linux, or Windows operating system.

13.1 Access Problems

13.13.1.1 Why can't I access the SMH pages, when Microsoft Service Console (MSC) shows the SMH service as running?

When the SMH is not responding and the SMH processes stop unexpectedly, the **Event Viewer** might display the following messages: `The HP System Management Homepage Win32 service has stopped successfully. HP System Management Homepage Service has stopped unexpectedly.`

The workaround is to restart the SMH service.

13.13.1.2 SMH Documentation Unclear on Treatment of securetty.

The HP System Management Homepage (HP SMH) does not use `/etc/securetty`. See *login*(1) for details on `/etc/securetty`.

13.13.1.3 After entering a hostname on Linux, HP SMH does not start.

Hostnames that are 64 characters or longer in length are not supported on Linux.

13.13.1.4 I am unable to access the HP SMH system, displays `Firewall is blocking your application`.

On latest Windows systems, by default, firewall settings are enabled.

Complete the following steps to change the firewall settings on a system running either on Windows 2003 or Windows 2008 operating systems.

1. From **Start**, go to **Control Panel**, select **Windows Firewall**.
2. Click on the **Change settings** link.
3. In the **General** tab, uncheck the checkbox **Block all Incoming Connections**, if it is enabled.
4. In the **Exceptions** tab, double-click **Add Program** button.

   Add a Program dialog box appears.
5. Click **Browse** button and navigate to `C:/hp/hpsmh/bin/` location. Select **hpsmhd**, and click **Open** button.
6. Apply **OK**.

Complete the following steps to change the firewall settings on a system running on Windows 2008 R2 operating system:

1. From **Start**, go to **Control Panel**, and then go to **System and Security** and click **Windows Firewall** option.

   The **Windows Firewall** page appears.
2. Select **Advanced settings** on the **Windows Firewall** page.
3. Click on **Inbound rules**, and on the **Actions** pane, click on **New rule**.

   The **New Inbound Rule Wizard** appears.
4. In the **actions** section, click on **New rule**.
5. On the **Rule Type** screen, select Rule Type as **Port**, and click **Next**.
6. On the **Protocols and Ports** screen, select **TCP** and enter 2301 and 2381 as specific local ports, and click **Next**.
7. On the **Action** screen, select **Allow the connection**, and click **Next**.

8. On the **Profile** screen, check all the three rules: **domain**, **private**, and **public** checkboxes.
9. Enter the Name the rule in the **Name** field and **Description**, which is optional, and click **Finish**.

13.2 Browser Problems

13.13.2.1 When I sign into HP SMH and close the browser, the HP SMH session is not ended. If I reopen Internet Explorer, after closing it I can sign into HP SMH without credentials. How can I fix this problem?

There are two possible solutions in order to be sure the HP SMH shortcut asks for credentials.

Solution 1

1. Select **Tools Internet Options**
2. Choose the **Advanced** tab.
3. Under **Settings Browsing**, deselect **Reuse windows for launching shortcuts (when tabbed browsing is off).**
4. Click **OK**.

Solution 2

1. Select **Tools Internet Options**
2. Under the **General** tab, look for **Tabs: Change how webpages are displayed in tabs**. Click **Settings**.
3. Under **Open links from other programs in:**, select the third option **The current tab or window**.
4. In the **Tabbed Browsing Settings** pop-up window, click **OK**.
5. Click **OK** to close **Internet Options**.

13.13.2.2 When I use Internet Explorer 6.0 in Windows, why do I see warnings in the **Security Alert** dialog box when I sign in to the HP System Management Homepage (HP SMH)?

There are two possible warnings:

- Warning 1: `The name on the security certificate is invalid or does not match the name of the site.`

  This warning occurs when you browse to HP SMH using an IP address. This warning also occurs if you browse locally using localhost for the machine name.

- Warning 2: `The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the CA.`

  The certificate is issued by HP SMH. You can add the certificate to your **Trusted Certificate List** and the warning goes away.

13.13.2.3 Opening a second Mozilla browser can appear as an unauthorized sign-in into HP SMH.

Mozilla browsers share sessions when launched separately.

Separate sessions are shared in Mozilla when launched from the desktop. However they are not shared in Internet Explorer.

13.13.2.4 I get security messages or partially displayed pages when browsing into HP SMH from Internet Explorer running on Windows 2003.

Internet Explorer 6.0 on Windows 2003 Server has different default security settings. To prevent the problem, add each managed system to the local intranet zone twice, once as **`http://`*`hostname`*`:2301`** and once more as **`https://`*`hostname`*`:2381`**. The alternatives to this solution are to decrease the level of security settings in the

browser (not recommended) or alter the browser security settings to allow cookies (both stored and per-session) and allow active scripting.

13.13.2.5 My browser page does not display all contents. What is wrong?

Frame sizes are optimized for medium fonts. If you switch your browser to use larger or smaller fonts, manually adjust the frame layout using the mouse.

13.13.2.6 Why does the browser prompt me to accept cookies when accessing a system?

Browser cookies are required to track user state and security. Cookies must be enabled in the browser and prompting for acceptance of cookies should be disabled.

13.13.2.7 When I browse to **`https://ipaddress:2381`** on a local machine or a remote machine running Windows 2003, I don't see the **Sign in** screen.

Internet Explorer 6.0 on Windows 2003 sometimes causes only the **Account Sign in** text in a blue bar to appear, instead of the entire **Sign in** page. This issue occurs when browsing on a local system or a remote system.

To resolve the issue, enable Javascript support and add this site to the Trusted sites list.

13.3 Installation Problems

13.13.3.1 After running `setup.exe /r` on a Windows system to import certificates, the installation fails.

Do not use `setup.exe /r` to import or copy certificates. Instead, use the **Configure or Repair Agents** tool in HP SIM.

13.13.3.2 When installing HP SMH, I receive the following error: `another instance is running.`

The HP SMH installation attempted to install on a system that had files that are corrupted, or the installation was aborted.

To resolve this issue, navigate to the `\temp` directory on the HP SMH system and delete the `smhlock.tmp` file.

13.13.3.3 When installing HP SMH, I receive the following errors: `error: cannot get exclusive lock on /var/lib/rpm/Packages error: cannot open Packages index using db3 - Operation not permitted (1) error: cannot open Packages database in /var/lib/rpm.`

This error appears when more than one instance of the install action is initiated on a Linux system. Only one HP SMH installation can run at a time.

13.4 IP Address Problems

13.13.4.1 Why do I get a security warning when I browse to HP SMH with an IPv6 address?

To use IPv6 addresses, you need the following browsers:

- **Windows OS**

  Mozilla Firefox and Internet Explorer 7or later

- **Linux OS**

  Mozilla Firefox

Note: Internet Explorer 6 cannot handle IPv6 addresses. For more information, see http://blogs.msdn.com/ie/archive/2007/02/20/ipv6-uris-in-ie7.aspx and the Microsoft support page at http://support.microsoft.com/kb/325414.

When browsing secure pages, Internet Explorer 7 might ask you to add the page to its Trusted Site Zone. Even clicking **Add**, the message returns. In this case, Internet

Explorer 7 fails to handle IPv6 URLs since the Internet Explorer parser uses a colon as the separator of the IP address and the Port number. For example,

- On IPv4, the HP SMH IP address might be **`https://127.0.0.1:2381`**. The IP address is 127.0.0.1 and the port number is 2381.
- On IPv6, the HP SMH IP address might be **`https://[2001:db8:c18:1:21a:4bff:fe4c:c8e0]:2381`**. The IP address is 2001:db8:c18:1:21a:4bff:fe4c:c8e0 and the port number is 2381 in this case, Internet Explorer looks for a colon as a separator and uses [2001 as the IP address.

Choose one of two ways to avoid security warnings when browsing with IPv6 addresses:

- Use a DNS name backed by IPv6 addresses.
- Add the literal IPv6 address to the Local intranet site or Trusted sites of Internet Explorer 7 without the port number. For example, add **`http://[2001:db8:c18:1:250:8bff:fee2:4ed8]`** and **`https://[2001:db8:c18:1:250:8bff:fee2:4ed8]`** without adding the port number.

13.13.4.2 Is there an easier way to access the local system with my browser without finding out its IP address?

Yes. You can access the local system at **`https://hostname:2381`** or **`https://127.0.0.1:2381`**. For HP-UX, you can access the local system at **`http://hostname:2301`** if you keep the default setting of `autostart` enabled.

NOTE: The word *localhost* does not work in all languages. In addition, if you have a proxy server configured in your browser, you might need to add 127.0.0.1 to the browser list of addresses that should not be proxied.

13.13.4.3 When I use the **IP Restricted Login** feature, entering my server IP address does not have the desired effect. How can I be sure that the local machine IP addresses are recognized by this feature?

Enter 127.0.0.1 in addition to the IP addresses of the server if you intend to restrict the local machine. The address 127.0.0.1 is always permitted in the **Include** section, so it is only restricted if it is explicitly placed in the **Exclude** section.

13.13.4.4 Although an IP restriction is configured, localhost access is not being denied. Why is this happening?

If you do not include the IP address for the local host in the Include field, the local host is still granted access because most users do not intend to block local host access. If you **do** need to block localhost access, enter **`127.0.0.1`** into the **Exclude** field under **IP Restriction**.

13.13.4.5 Under **IP Restriction**, I did not include the system's local IP address or 127.0.0.1 to the **Include** list, but I can still browse to it locally.

As a precaution against users unintentionally locking themselves out of HP SMH access, localhost requests are not denied when the local IP addresses are not mentioned in the **Include** list. If necessary, the local system's IP address and 127.0.0.1 can be added to the **Exclude** list, and this setting denies access to any user trying to gain access from the local system.

13.5 Sign In Problems

13.13.5.1 I am unable to do an SSO from HP Systems Insight Manager to HP System Management Homepage?

When a CA certificate is used, you might be unable to do an SSO from HP SIM to HP SMH v7.0.0 onwards. The following error message is displayed on the SMH login page `Trusted certificate used for SSO is either revoked`

`or SMH failed to verify it against CRL`. In such a case, you have to manually log in to SMH.

To use a CA Certificate for SSO, follow the prerequisites listed here to:

- Create a certificate request
- Get the signed certificate from CA
- Get the Root Certificate and the CRL from CA
- Import the signed certificate in SIM
- Set up SMH
- Configure on SMH system

Create a certificate request:

1. Log in to SIM.
2. Select **Options→Security→HP System Insight Manager Server Certificate**.
3. Click **Import**.
4. Click **more…** at the end of first option **Create a Certificate Signing Request (CSR)**.
5. Click **Create** to download PKCS 10 certificate file and save it.
6. Submit the certificate request to CA to get a signed certificate.

Get the signed certificate from CA:

NOTE: You can also set up local certificate services such as Microsoft Certificate Services to get the signed certificate.

1. Access **`http://hostname/certsrv`**, where *`hostname`* is the name of the machine having certificate services.
2. Select **Request a certificate**.
3. Select **Advanced certificate request**.
4. Select **Submit a certificate request by using a base-64-encoded CMC**, **PKCS #10 file**, or **Submit a renewal request by using a base-64-encoded PKCS #7 file**.
5. To download a certificate that is pending for approval:
   a. Access **`http://hostname/certsrv`**, where *`hostname`* is the name of the machine having certificate services.
   b. Click **View the status of a pending certificate request** and download the signed certificate to save it.

Get the Root Certificate and the CRL from CA:

NOTE: You can also set up local certificate services such as Microsoft Certificate Services to get the Root Certificate and the CRL.

1. Access **`http://hostname/certsrv`**, where *`hostname`* is the name of the machine having certificate services.
2. Select **Download a CA certificate**, **certificate chain**, or **CRL**.
3. Select **Base64** as encoding method.
4. Select **Download a CA certificate**.
5. Click **Save**.
6. Click **Download latest base CRL**.
7. Click **Save** to save the CRL.

Import the signed certificate in SIM:

1. Log in to SIM.

2. Select **Options** →**Security**→**Credentials**→**Trusted Systems**.
3. Select **Trusted Certificates** tab.
4. Click **Import**.
5. Browse to select **root CA certificate file**.
6. Click **OK**. The root CA certificate will be added to Trusted Certificates.
7. Select **Options** →**Security**→**HP System Insight Manager Server Certificate**.
8. Click **Import**.
9. Click **more…**at the end of the third option **Import signed certificate reply from CA**.
10. Browse to select **signed certificate** file.
11. Click **Import**.

Set up SMH:

1. Log in to the console of the SMH system.
2. Select **Settings**→**SMH** →**Security** →**Trusted Management Servers**.
3. Select **Get Certificate Information**, provide the server name or the IP address of the SIM machine.
4. Click **Add certificates** to add the certificate to the trusted certificate list.

Configure on SMH system:

1. Log in to the console of the SMH system.
2. Create a directory; for example, `c:\cafiles`.
3. Create two subfolders **cacerts** and **cacrls**.
4. Place the root and the intermediate certificates in the **cacerts** directory.
5. Place CRLs in the **cacrls** directory.
6. Enter the command `smhconfig -W c:\cafiles` to set the `cafiles` path and then execute `smhconfig -r`.

NOTE: The `smhconfig -W ""` will completely disable the CA revocation check.

After SMH is configured to use the CA, SMH accepts SSO requests from SIM.

- To revoke a certificate:
  1. Log in to the console of the Certificate Service machine.
  2. Click the **Issued Certificates** folder.
  3. Right-click the certificate to be revoked, **All Tasks**→**Revoke certificate**.
  4. After revoking the certificate publish the CRL.
- To publish a CRL:
  1. Log in to the console of the Certificate Service machine.
  2. Right-click the **Revoked Certificates** folder, or option and select **All Tasks** →**Publish**.

     NOTE: You must use the latest CRL for certificate verification.

13.13.5.2 After signing onto the Windows operating system on a ProLiant or Integrity server running HP SMH Version 2.1.3 (or later), the ROTATELOGS.EXE command prompt appears on the screen if SMH is configured to allow interaction with the desktop. When this occurs, one or two smaller command prompt windows appear with messages similar to the following:

```
(drive) :\hp\hpsmh\bin\rotatelogs.exe
```

The command prompt window messages do not affect the performance or functionality of the server or of SMH and can be ignored.

Any ProLiant or Integrity server configured with Windows 2000 Server or Windows Server 2003 (any edition) and HP SMH Version 2.1.3 (or later) when SMH is allowed to interact with the desktop can be affected.

To prevent HP SMH from interacting with the server desktop, perform the following:

1. Click **Start→Programs→Administrative Tools→Services**
2. Click HP System Management Homepage **Properties**.
3. Click the **Log On** tab.
4. Deselect **Allow service to interact with desktop**.
5. Click **Apply** and then click **OK**.
6. Restart the HP System Management Homepage service.

13.13.5.3 I gave a user group defined by Windows, such as **Backup Operators**, **Administrator**, **Operator** and **User** , privileges through the HP SMH **User Groups** settings page. However, users in that group cannot sign in or do not have the correct privileges in HP SMH.

HP SMH only recognizes four user groups defined by Windows: **Administrators**, **Users**, **Guests** and **Power Users**. Other groups defined by Windows, such as **Backup Operators**, are not recognized.

NOTE: On Linux, the group must be previously created using system tools as groupadd.

13.13.5.4 When trying to sign in to HP SMH on a Windows system using an administrative account defined in the **Backup Operators** group, the sign in fails.

On Windows systems in the defined user groups, only **Administrators**, **Users**, **Guests** and **Power Users** are recognized. Other groups defined by Windows, such as **Backup Operators**, are not recognized. Create a new group and use it for providing access to HP SMH.

13.13.5.5 I cannot sign in to HP SMH on my server running the Windows operating system.

Complete the following:

1. Verify that a valid Windows operating system account is set up and that the sign-in is included in the **Administrators** group or in an HP SMH operating system group.
2. Sign in to the operating system, and change the password if prompted.

   If this password prompt appears, the operating system Administrator has set up the user account with the **user must change the password at next sign in option** selected.

   Any sign-in created in the future can be added by the operating system group Administrator without selecting the **user must change the password at next sign on** option. In addition, if this option is selected, you can change the password through the operating system before signing in to HP SMH.

13.13.5.6 I cannot sign in to HP SMH on my Windows XP operating system.

Go to **Programs→Administrative Tools→Local Security Settings** and change the policy to **Network Access: Sharing and security model for local accounts** from **Guest Only** to **Classic Only**.

13.13.5.7 Why doesn't my password work after I upgrade my web-managed Products?

HP SMH v2.0 and later use operating system accounts, but previous versions use static accounts (**administrator**, **operator**, and **user**). Any operating system account belonging to the administrators group (root group in Linux) has administrative access to HP SMH. With this access, you can assign accounts in other operating system

account groups to different levels of access for HP SMH. The HP SMH online help describes this process in detail.

NOTE: This does not apply to HP-UX.

13.13.5.8 I created new Windows accounts, using default settings, for use with HP SMH but I cannot use them to sign in.

By default, new accounts created in Windows operating systems are set to **user must change the password at next sign in**. Deselect this option so the account can be used to sign in to HP SMH.

13.13.5.9 When I use Internet Explorer 6.0 in Windows and browse through the management server to a system that was discovered by IP address, I cannot sign in to HP SMH. If anonymous access is enabled, I get through anonymously but the user name is incorrect.

or

When I use Internet Explorer 6.0 in Windows and browse through the management server to a device that was discovered by IP address, the detailed certificate information does not appear in the text box of the **Automatic Import Certificate** screen.

These issues can be resolved in the following ways by adjusting the Internet Explorer settings:

- Configure the **Internet Explorer Privacy** settings from **Medium** to **Low**. (HP does not recommend using this option.)

  To change the settings:

  1. In Internet Explorer, click **Tools** → **Internet Options**.
  2. Click **Privacy**.
  3. Click and drag the slide bar to **Low**.
  4. Click **Apply**.
  5. Click **OK**.

     The changes are saved.

- Add the IP address of the target HP SMH to the Local Intranet's zone.

  To change the settings:

  1. In Internet Explorer, click **Tools** → **Internet Options**.
  2. Click **Security**.
  3. Select **Local Intranet**.
  4. Click **Sites** → **Advanced**.
  5. In **Add this website to the zone**, enter the IP address of the HP SMH system for example, enter `https://ipaddress` .
  6. Click **Add**.
  7. Click **OK**.
  8. Click **OK** again.
  9. Click **OK**.

     The changes are saved.

13.13.5.10 When I browse to my system using the server name `http://my-server-name:2301` with Internet Explorer, I cannot sign in using my valid Windows administrator account username and password. However, I can sign in if I browse to my system using my IP address, `http://my-ip-address:2301`.

Verify whether there is an underscore "_" defined in your server's computer name. If there is, remove it or use "-" (dash) instead of "_" (underscore). You should be able to log in using the system name.

NOTE: You might need to change the Microsoft Internet Information Server (IIS) configuration after you rename a system.

This is a security feature added by Microsoft security patch MS01-055 for Internet Explorer 5.5 or 6.0 that prevents systems with improper name syntax from setting cookie names. Domains that use cookies must use only alphanumeric characters (- or .) in the domain name and the system name. Internet Explorer blocks cookies from a system if the system name contains other characters, such as an underscore character (_).

13.6 Security Problems

13.13.6.1 After updating my Windows XP system with Service Pack 2, I cannot access HP SIM or HP Version Control Repository Manager. What happened?

Windows XP Service Pack 2 implements a software firewall that prevents browsers from accessing the ports required for HP SIM and HP Version Control Repository Manager access. To resolve this issue, configure the firewall with exceptions to allow browsers to access the ports used by HP SIM and HP Version Control Repository Manager.

HP recommends the following actions:

1. Select **Start→Settings Control Panel.**
2. Double-click **Windows Firewall** to configure the firewall settings.
3. Select **Exceptions**.
4. Click **Add Port**.
5. Enter the product name and the port number.

   Add the following exceptions to the firewall protection:

Table 9 Firewall protection exceptions

Product	Port Number
HP SMH Insecure Port:	2301
HP SMH Secure Port:	2381
HP SIM Insecure Port:	280
HP SIM Secure Port:	50000

6. Click **OK** to save your settings and close the **Add a Port** dialog box.
7. Click **OK** to save your settings and close the **Windows Firewall** dialog box.

This configuration leaves the default SP2 security enhancements intact, but allows traffic over the ports previously indicated. These ports are required for HP SIM and HP Version Control Repository Manager to run. Ports 2301 and 2381 are required for the HP Version Control Repository Manager and ports 280 and 50000 are required by HP SIM. The secure and insecure ports must be added for each product to enable communication with the applications.

13.13.6.2 Why can't I import X.509 certificates directly into HP SMH?

HP SMH generates Certificate Request in Base64-encoded PKCS #10 format. This certificate request should be supplied to the certificate authority. Most CAs return Base64-encoded PKCS #7 certificate data that you can import directly into HP SMH

by selecting **Settings→HP System Management Homepage→Security→Local Server Certificate**.

If the CA returns the certificate data in X.509 format, rename the X.509 certificate file as `cert.pem` and place it into the `\hp\sslshare` directory. When HP SMH is restarted, this certificate is used.

13.13.6.3 Why is my PKCS #7 cert data not accepted?

When using a Mozilla browser, there can be problems when cutting and pasting cert request and reply data using Notepad or other editors. To avoid these problems, use Mozilla to open certificate reply files from your CA. Use the Select All, Cut, and Paste operations supplied by Mozilla when working with certificates.

13.13.6.4 Why is my private key file not protected by the file system?

If you are using Windows operating systems, you must have the system drive in NTFS format for the private key file to be protected by the file system.

13.13.6.5 Why do I get errors when I paste my customer-generated certificate PKCS #7 data into the HP SIM Certificate Data field in **Settings→HP SMH→Security→Trusted Management Servers**?

The customer-generated certificate PKCS #7 data is not relevant to the date given in the **Trusted Management Servers** field. The **PKCS #7** data should be imported into the **Customer Generated Certificates Import PKCS #7 Data** field under **Settings→HP SMH→Security→Local Server Certificate**. The **HP Systems Insight Manager Certificate Data** field is used to trust HP SIM servers with HP SMH.

13.13.6.6 Why can't I use a Windows 2003 CA to grant my third-party certificate into HP SMH?

To use a Windows 2003 CA to create a certificate for HP SMH:

1. Create the PKCS #10 data packet by clicking **Settings→HP SMH→Security→Local Server Certificate** page.
2. Press the **Ctrl**+ **C** keys to copy the data into a buffer.
3. Navigate to **`http://W2003CA/certsrv`** where *`W2003CA`* is the name of your Windows 2003 certificate authority system and complete the following:
   a. Select **Request a certificate**.
   b. Select **Advanced certificate request**.
   c. Select **Submit a certificate request by using a base**.
   d. Press the **Ctrl**+ **V** keys to paste the **PKCS #10** data into the field.
4. From your Windows 2003 certificate authority system complete the following:
   a. Click **Start→All Programs→Administrative Tools→Certification Authority**.
   b. Click **CA (Local)** ⇒ **W2003CA/certsrv** ⇒ where *`W2003CA`* is the name of your Windows 2003 certificate authority system.
   c. Issue the pending request certificate.
5. Navigate to **`http://W2003CA/certsrv`**, where *`W2003CA`* is the name of your Windows 2003 certificate authority system and complete the following:
   a. Select **View the status of a pending certificate request**.
   b. Select **Base64-encoded** and **Download certificate** (not **certificate chain**).
   c. The file download is `certnew.cer`.
   d. Rename `certnew.cer` to `cert.pem`.

13.7 Other Problems

13.13.7.1 I am having problems downgrading HP SMH from 3.x and above to 2.x.

To successfully downgrade HP SMH from 3.x and above to 2.x, stop the HP SMH service and execute the downgrade by completing the following steps:

1. `$/etc/init.d/hpsmhd stop`
2. `$rpm --oldpackage -U hpsmh-`*`old version`*`.rpm`

13.13.7.2 Why can't I install HP SMH on my system?

The HP SMH install action requires a Java version that requires at least 256 colors to load.

NOTE: This applies to Windows only.

13.13.7.3 Why do I get an error indicating the page cannot be displayed when I click the **Management Processor** link?

The administrator for the management processor has configured the Web server on the management processor to use a port other than port 80. HP SMH does not have access to that parameter and assumes the management processor is on port 80.

13.13.7.4 Why can't I install HP SMH on HP-UX or Linux when I am not root?

You must be logged in as root for HP SMH to have the proper access rights.

13.13.7.5 In the ServiceGuard Manager plugin, selecting **Display Consolidated Syslog** might require you to re-authenticate or cause a page not found error.

If the page not found error appears, press the **Refresh** button in the browser to allow the page to be shown. Subsequently, you need to reauthenticate.

13.13.7.6 Why does the Timeout error display on my system?

The Timeout error is displayed when a WebApp takes more time to load than the Timeout set in HP SMH.

To resolve, complete any or all of the following steps:

Increase the UI timeout by executing the command: `smhconfig -B 10-3600` or `smhconfig --ui-timeout [=] 10-3600`, where 10-3600 is the timeout range in seconds.

AND/OR

1. Browse through the SMH logs either locating **Logs→SMH→System Management Homepage Log** or execute the command: `\hp\hpsmh\bin\smhlogreader CLI` to find the agent(s)/WebApp(s) which is causing the timeout issue.
2. Disable the problematic agent(s)/webapp(s), either uninstalling the agent(s)/WebApp(s) or moving the `.xml` file from the WebApp directory.
3. Restart the HP SMH service.

14 Service and support

Support for HP SMH is provided as an adjunct to support of the underlying hardware. The HP Support pages provide you with a variety of product, service, and support-related resources for HP SMH.

- Access HP SMH on the Software Depot home. Go to http://www.hp.com/go/softwaredepot and select **Security and manageability**. Look for the **HP System Management Homepage** link. The support for Linux Integrity is found by selecting the Linux link on Software Depot home. Look for the **HP Integrity Essentials Pack for Linux** link.
- Access the HP ProLiant Essentials software page at http://www.hp.com/servers/manage. You find a wealth of Systems Management Products and service-related information.
- Access the HP Support Center for maintenance and support, forums, and training and education of HP products at http://www.hp.com/go/hpsc.
- Contact the HP Support Center Forum to get answers to your HP product questions at http://www.hp.com/go/hpsc.

Keeping good records of your configuration can significantly speed up the troubleshooting process. Keep current and consult the following list when you obtain assistance from your HP service provider:

- Management system make, model, and serial number information
- Operating system information, operating environment information (HP-UX), including version number, a list of service packs applied, patches, the Compaq SSD version, and Insight Agents' names and versions that have been applied
- Hardware configuration information for Linux and Windows:
  - Survey Utility output or Inspect printout
  - System Configuration Utility printout
  - Description of non-HP or non-Compaq equipment that is not shown on the Inspect or System Configuration printout

Support and other resources

Information to collect before contacting HP

Be sure to have the following information available before you contact HP:

- Software product name
- Hardware product model number
- Operating system type and version
- Applicable error message
- Third-party hardware or software
- Technical support registration number (if applicable)

How to contact HP

Use the following methods to contact HP technical support:

- In the United States, see the Customer Service / Contact HP United States website for contact options:

  http://welcome.hp.com/country/us/en/contact_us.html

- In the United States, call 1-800-HP-INVENT (1-800-474-6836) to contact HP by telephone. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, conversations might be recorded or monitored.
- In other locations, see the Contact HP Worldwide website for contact options:

  http://welcome.hp.com/country/us/en/wwcontact.html

Security bulletin and alert policy for non-HP owned software components

Open source software (such as OpenSSL) or third-party software (such as Java) are sometimes included in HP products. HP discloses that the non-HP owned software components listed in the Insight Management end user license agreement (EULA) are included with Insight Management. The EULA is included with the Insight Management Installer on Insight Management DVD #1.

HP addresses security bulletins for the software components listed in the EULA with the same level of support afforded HP products. HP is committed to reducing security defects and helping you mitigate the risks associated with security defects when they do occur.

When a security defect is found, HP has a well defined process that culminates with the publication of a security bulletin. The security bulletin provides you with a high level description of the problem and explains how to mitigate the security defect.

Subscription service

HP recommends that you register your product at the Subscriber's Choice for Business website:

http://www.hp.com/country/us/en/contact_us.html

After registering, you will receive email notification of product enhancements, new driver versions, firmware updates, and other product resources.

Registering for software technical support and update service

Insight Management includes one year of 24 x 7 HP Software Technical Support and Update Service. This service provides access to HP technical resources for assistance in resolving software implementation or operations problems.

The service also provides access to software updates and reference manuals in electronic form as they are made available from HP.

With this service, Insight Management customers benefit from expedited problem resolution as well as proactive notification and delivery of software updates. For more information about this service, see the following website:

http://www.hp.com/services/insight

Registration for this service takes place following online redemption of the license certificate.

How to use your software technical support and update service

As HP releases updates to software, the latest versions of the software and documentation are made available to you. The Software Updates and Licensing portal gives you access to software, documentation and license updates for products on your HP software support agreement.

You can access this portal from the HP Support Center:

http://www.hp.com/go/hpsc

After creating your profile and linking your support agreements to your profile, see the Software Updates and Licensing portal at http://www.hp.com/go/hpsoftwareupdatesupport to obtain software, documentation, and license updates.

HP authorized resellers

For the name of the nearest HP authorized reseller, see the following sources:

- In the United States, see the HP U.S. service locator web site:

  http://www.hp.com/service_locator
- In other locations, see the Contact HP worldwide web site:

  http://www.hp.com/go/assistance

New and changed information in this edition

To review what is new and changed in this release of HP SMH, see the *HP System Management Homepage Release Notes* on the HP Technical Documentation website at http://www.hp.com/go/insightmanagement/sim/docs.

Related Documents

Documents

- ***HP System Management Homepage Release Notes***

  The release notes provide documentation for what's new with the release, features and change notifications, system requirements, and known issues. The release notes are available on the HP Technical Documentation website at http://www.hp.com/go/hpux-core-docs, select HP-UX System Administration for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the release notes is available at the HP SMH web page at http://www.hp.com/go/insightmanagement/sim/docs.
- **HP System Management Homepage Help System**

  The help system provides a complete set of documentation for using, maintaining, and troubleshooting HP SMH. In HP SMH, go to the **Help** menu.
- ***HP System Management Homepage Installation and Configuration Guide***

  The installation guide provides information about installing and getting started using HP SMH. It includes an introduction to basic concepts, definitions, and functionality associated with HP

SMH. The installation guide is available on the HP Technical Documentation website at http://www.hp.com/go/hpux-core-docs, select HP-UX System Administration for the latest documents and for previous versions of the documents, select either HP-UX 11i v1 or HP-UX 11i v2. Also, for Linux and Windows operating system releases, the installation guide is available at the HP SMH web page at http://www.hp.com/go/insightmanagement/sim/docs.

- **Next generation single-system management on HP-UX 11i v2 (B.11.23)**

  This white paper introduces HP SMH and its various plug-ins. The use cases involving HP SMH plug-ins highlight the features provided by HP SMH. The white paper is available on the HP Technical Documentation website at http://www.hp.com/go/hpux-core-docs select HP-UX 11i v2 and search with the document title "Next generation single-system management on HP-UX 11i v2 (B.11.23)."

- ***hpsmh* (1m) manpage**

  For HP-UX releases, the manpage is available from the command line using the `man hpsmh` command. This information is not available for Linux and Windows operating systems.

- ***smhstartconfig* (1M) manpage**

  For HP-UX operating system releases, the manpage is available from the CLI using the `man smhstartconfig` command. This information is not available for Linux and Windows operating systems.

- ***sam*(1M) manpage**

  For HP-UX operating system releases, the manpage is available from the CLI using the `man sam` command. This information is not available for Linux and Windows operating systems. Note: SAM functionality changes in http://h18013.www1.hp.com/products/servers/management/agents/documentation.html.

- ***smh* (1m) manpage**

  This command is available in HP-UX 11i v3 (B.11.31) only. This is an enhanced version of the *sam*(1m) command. For HP-UX operating system releases, the manpage is available from the CLI using the `man smh` command. This information is not available for Linux and Windows operating systems.

Websites

- HP System Management Homepage website

  The website provides HP SMH information and product links. Go to the HP website at http://www.hp.com or to the Software Depot home at and search for System Management Homepage.

- HP Insight Essentials software page

  This web page is at http://www.hp.com/servers/manage.

Typographic conventions

This document uses the following typographical conventions:

Book title	The title of a book. On the web, this can be a hyperlink to the book itself.
`Command`	A command name or command phrase, for example `ls -a`.
`Computer output`	Information displayed by the computer.
Ctrl+x or **Ctrl-x**	A key sequence that indicates you must hold down the keyboard key labeled **Ctrl** while you press the letter `x`.
`ENVIRONMENT VARIABLE`	The name of an environment variable, for example, `PATH`.

Key	The name of a keyboard key. **Return** and **Enter** both refer to the same key.
Term	A term or phrase that is defined in the body text of the document, not in a glossary.
`User input`	Indicates commands and text that you type exactly as shown.
find(1)	HP-UX manpage. In this example, “find” is the manpage name and “1” is the manpage section.
`Replaceable`	The name of a placeholder that you replace with an actual value.
[ ]	In command syntax statements, these characters enclose optional content.
{ }	In command syntax statements, these characters enclose required content.
|	The character that separates items in a linear list of choices.
…	Indicates that the preceding element can be repeated one or more times.
WARNING	An alert that calls attention to important information that, if not understood or followed, results in personal injury.
CAUTION	An alert that calls attention to important information that, if not understood or followed, results in data loss, data corruption, or damage to hardware or software.
IMPORTANT	An alert that calls attention to essential information.
NOTE	An alert that contains additional or supplementary information.
TIP	An alert that provides helpful information.

A HP SMH file locations

Table 10 HP SMH file locations

Description	Windows	Linux	HP-UX
HP SMH Root The root of the HP SMH installation.	*SystemDrive*\hp\hpsmh	/opt/hp/hpsmh	/opt/hpsmh
HP SMH Executable The HP SMH binary. A webapp can use detection of this file's presence to verify that HP SMH is installed on the system.	*SystemDrive*\hp\hpsmh\bin\hpsmhd.exe	/opt/hp/hpsmh/sbin/hpsmhd	/opt/hpsmh/lbin
Certificate and Key files The certificate and private key files used by HP SMH. This is a shared location used by a number of management applications. The keys may be either 1024 or 2048 bits.	*SystemDrive*\hp\sslshare\cert.pem *SystemDrive*\hp\sslshare\file.pem	/etc/opt/hp/sslshare/cert.pem /etc/opt/hp/sslshare/file.pem	/opt/hpsmh/sslshare
HP SMH XML configuration This file should only be modified by HP SMH itself.	*SystemDrive*\hp\hpsmh\conf\smhpd.xml	/opt/hp/hpsmh/conf/smhpd.xml	/opt/hpsmh/conf.common/smhpd.xml
HP SMH conf file The conf file is regenerated at every startup and modification of the version on disk.	*SystemDrive*\hp\hpsmh\conf\smhpd.conf	/opt/hp/hpsmh/conf/smhpd.conf	/opt/hpsmh/conf
2381 Document Root The root for documents served on port 2381 (HTTPS).	*SystemDrive*\hp\hpsmh\data\htdocs	/opt/hp/hpsmh/data/htdocs	/opt/hpsmh/data/htdocs
2301 Document Root The root for documents served on port 2301. Security restrictions allow only particular HP SMH documents to be served out of this directory (HTTP).	*SystemDrive*\hp\hpsmh\data\isdocs	/opt/hp/hpsmh/data/isdocs	/opt/hpsmh/data/isdocs
cgi-bin Root The root of executable content.	*SystemDrive*\hp\hpsmh\data\cgi-bin	/opt/hp/hpsmh/data/cgi-bin	/opt/hpsmh/data/cgi-bin

Table 10 HP SMH file locations *(continued)*

Description	Windows	Linux	HP-UX
Help Root The root where help files are placed.	*SystemDrive*\hp\hpsmh\data\help	/opt/hp/hpsmh/data/help	/opt/hpsmh/data/help
Webapp XML files The root where webapp XML configuration files are placed.	*SystemDrive*\hp\hpsmh\webapp	/opt/hp/hpsmh/webapp	/opt/hpsmh/webapp

B HP SMH Ciphers

Ciphers used in HP SMH

This appendix provides a list of all the Ciphers used in the HP SMH product.

Table 11 Ciphers used in HP SMH

Cipher	Syntax	Description	Directive used in HP SMH	Description
SSLProtocol	SSLProtocol [+|-]protocol ...	Configure usable SSL protocol flavors	SSLProtocol all -SSLv2	Enable SSLv3 and TLSv1, but not SSLv2. **NOTE:** All includes SSLv3, TLSv1, and SSLv2.
SSLCipherSuite	SSLCipherSuite cipher-spec	Cipher Suite available for negotiation in SSL handshake	SSLCipherSuite ALL:!ADH:!EXPORT56: !EXPORT40:RC4+RSA: +HIGH:+MEDIUM:-SSLv2 :+EXP:-LOW:-eNULL	Enable All except ADH, EXPORT56, EXPORT40, SSLv2, LOW, eNULL, and enable RC4, RC2, HIGH, MEDIUM, and EXP. **NOTE:** where: • ADH: all ciphers using Anonymous Diffie-Hellman key exchange • EXPORT56: all 56-bit export ciphers only • EXPORT40: all 40-bit export ciphers only • SSLv2: all SSL version 2.0 ciphers • LOW: all low strength ciphers [no export, single DES] • RC4: RC4 encoding ciphers • RSA: all ciphers using RSA key exchange • HIGH: all ciphers using Triple-DES • MEDIUM: all ciphers with 128-bit encryption • EXP: all export ciphers • eNULL: No encoding ciphers

15 Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.

Glossary

Accounts for Users & Groups tool (ugweb) The HP-UX Accounts for Users and Groups (ugweb) tool is used to manage user accounts and group accounts on the local system. This tool can also be used to manage user accounts on a NIS system. The ugweb tool can be launched from the HP-UX System Administration Manager (SAM) tool or from HP SMH.

AS *See* Kerberos Authentication Server.

CA *See* certificate authority.

caution A note to indicate that failure to follow directions could result in damage to equipment or loss of information.

certificate An electronic document that contains a subject's public key and identifying information about the subject. The certificate is signed by a certificate authority (CA) to bind the key and subject identification together.

certificate authority (CA) A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual who has been granted the unique certificate is the individual he or she claims to be.

CLI *See* command line interface.

command line interface (CLI) The set of commands that you can execute directly from the command shell of an operating system.

Disks and File Systems tool (fsweb) The HP-UX Disks and File Systems (fsweb) tool is used to manage file systems, logical volumes, and disks. The Disks and File Systems tool can be launched from the HP-UX System Administration Manager (SAM) tool or from HP SMH.

DNS *See* Domain Name Service.

Domain Name Service (DNS) A service that translates domain names into IP addresses.

evweb *See* System Fault Management tool .

external sites Third-party application URLs.

fsweb *See* Disks and File Systems tool.

graphical user interface (GUI) A program interface that uses the graphics capabilities of a computer to make the program easier to use. The HP SMH GUI is Web-enabled and displays in a Web browser.

GUI *See* graphical user interface.

HP Insight Management Agent A program that regularly gathers information or performs some other service without the user's immediate presence.

HP SIM *See* HP Systems Insight Manager.

HP SMH *See* HP System Management Homepage.

HP System Management Homepage (HP SMH) The HP System Management Homepage (HP SMH) is a Web-based interface that consolidates and simplifies single system management for HP servers on HP-UX, Linux, and Microsoft Windows operating systems. By aggregating the data from HP Web-based agents and management utilities, HP SMH provides a common, easy-to-use interface for displaying hardware fault and status monitoring, performance data, system thresholds, diagnostics, and software version control for an individual server. HP SMH is an integrated piece of software used by the suite of HP Web-enabled System Management Software to communicate over HTTP and HTTPS. It provides a uniform set of functionality and security to HP Web-enabled System Management Software.

HP Systems Insight Manager (HP SIM) System management software that is capable of managing a wide variety of systems, including HP systems, clusters, desktops, workstations, and portables. HP SIM combines the strengths of HP Insight Manager 7, HP Toptools, and HP Servicecontrol Manager to deliver a single tool for managing HP ProLiant, HP Integrity, and HP 9000 systems running HP-UX, Linux, and Windows. The core HP SIM software delivers the essential capabilities required to manage all HP server platforms. HP SIM can also be extended to deliver unparalleled breadth of system management with plugins for HP storage, power, client, and printer products. Plugins for rapid deployment,

	performance management, and workload management enable systems administrators to pick the value added software required to deliver complete lifecycle management of their hardware assets. To obtain more information about HP SIM, go to http://www.hp.com/go/hpsim.
HP Version Control Agent (VCA)	An Insight Management Agent that is installed on a system to enable the customer to see the HP software installed on that server. The HP Version Control Agent can be configured to point to a HP Version Control Repository Manager, allowing easy version comparison and software update from the repository.
HP Version Control Repository Manager (VCRM)	An Insight Management Agent that allows a customer to manage HP-provided software stored in a user-defined directory/repository.
HP Web-enabled System Management Software	Software that manages HP Web-enabled products.
HP-UX System Administration Manager (SAM)	Is the primary interface for HP-UX 11i v1 (B.11.11) and HP-UX 11i v2 (B.11.23) system management. For HP-UX 11i v3 (B.11.31), HP SMH provides the primary interface for HP-UX system administration tasks. The legacy SAM functionality is still available.
HTTPS	*See* Secure HTTP.
in-place	Locally. For example to install in-place means to install locally.
Integrated Agents and Other Agents	The Integrated Agents area on the Tools page contains participants and links to their entry points if applicable. You can click an agent link to access that particular agent. Participants are agents that are contributing information contained in the HP System Management Homepage (HP SMH). If no HP Web-enabled System Management Software is installed that provides this information, then **none** is displayed. The Other Agents area on the Tools page lists the visible HP Web-enabled System Management Software that does not participate in HP SMH. The name of the HP Web-enabled System Management Software provides a link so that you can still access the agents if they provide a user interface. If no HP Web-enabled System Management Software is installed that provides this information, then **none** is displayed.
Integrity Support Pack	A set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. An Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.
Internet Protocol (IP) range	Systems with an IP address that falls in the specified range.
IP	*See* Internet Protocol (IP) range.
kcweb	*See* Kernel Configuration tool.
KDC	*See* Kerberos Key Distribution Center.
Kerberos	A trusted third-party authentication protocol developed at MIT which allows different hosts and users to authenticate and confirm the identity of each other.
Kerberos Authentication Server	A service whose sole purpose is to authenticate user account records. The AS serves as an introducer for the user and the service through the use of a shared secret key registered with the AS.
Kerberos Key Distribution Center	Kerberos Key Distribution Center, composed of the Authentication Server and the Ticket Granting Server.
Kerberos Ticket Granting Server	Adds an extra layer of indirection so that the user only needs to enter in a password once; the ticket and session key obtained from that password is used for all further tickets. Before accessing any regular service, the user requests a ticket from the Authentication Server (AS) to talk to the TGS. This ticket is called the *ticket granting ticket* or TGT; it is also sometimes called the *initial*

ticket. The session key for the TGT is encrypted using the user's long-term key, so the password is needed to decrypt it from the AS' response to the user.

Kernel Configuration tool (kcweb) The HP-UX Kernel Configuration (kcweb) tool is used to manage kernel tunables, modules and alarms. The Kernel Configuration tool can be launched from the HP-UX System Administration Manager (SAM) tool or from HP SMH

MIT Massachusetts Institute of Technology.

multihomed Multiple names set to a certificate.

parMgr *See* Partition Manager.

Partition Manager (parMgr) Provides system administrators with a convenient GUI to configure and manage nPartitions on HP server systems. Perform complex configuration tasks without having to remember commands and parameters. Select nPartitions, cells, I/O chassis, or other components from the graphical display, then select an action from a menu. You can use Partition Manager to perform the following tasks: create, modify, and delete nPartitions; examine the nPartition configuration of a complex, check the complex for potential configuration and hardware problems, and manage hardware resources on the complex.

NOTE: At this time, HP System Management Homepage does not support Partition Manager.

pdweb *See* Peripheral Device tool.

Peripheral Device tool (pdweb) The HP-UX Peripheral Device (pdweb) tool can be used to easily and quickly view I/O devices and OLRAD cards. It helps manage hot pluggable PCI slots on systems that support adding and replacing cards without rebooting. On all HP-UX systems, pdweb displays the I/O devices and can be used to (re)create device files for a selected device. The Peripheral Device tool can be launched the HP-UX System Administration Manager (SAM) tool or from HP SMH.

PKI *See* Public Key Infrastructure.

Principal Users or service / host which are present in a Kerberos realm and are allowed to authenticate to each other.

ProLiant or Integrity Support Pack A set of HP software components that have been bundled together by HP, and verified to work with a particular operating system. A ProLiant or Integrity Support Pack contains driver components, agent components, and application and utility components. All of these are verified to install together.

Public Key Infrastructure (PKI) Public Key Infrastructure is the combination of software, encryption technologies, and services that enables enterprises to protect the security of their communications and business transactions on the Internet.

Realm Kerberos domain. Usually, it is the network's domain name in capital letters. For example, the Kerberos realm for the smhkerberos.com would conventionally be called `SMHKERBEROS.COM`.

Red Hat Package Manager (RPM) The Red Hat Package Manager is a powerful package manager that can be used to build, install, query, verify, update, and uninstall individual software packages. A package consists of an archive of files and package information, including name, version, and description.

repository The database that stores vital information about the managed cluster, including users, nodes, node groups, roles, tools, and authorizations.

RPM *See* Red Hat Package Manager.

SAM *See* HP-UX System Administration Manager.

search criteria A set of variables (information) used to define a requested subset of information from the set of all information. The information set that can be filtered includes action information, some of the system's information, and so on. A filter is composed of an permitted filter followed by a restricted filter. The result of these two filtering operations is called a group. An example of a filter is a SQL statement that creates viewable information or causes management operations to be performed.

Secure HTTP (HTTPS) An extension to the HTTP protocol that supports sending data securely over the Web.

Secure Shell (SSH) A program that enables you to sign in to another system over a network and execute commands on that system. It also enables you to move files from one system to another, and it provides authentication and secure communications over insecure channels.

Secure Sockets Layer (SSL)	A standard protocol layer that lies between HTTP and TCP and provides privacy and message integrity between a client and server. A common use of SSL is to provide authentication of the server, so the client can be assured it is communicating with the system that the system claims to be. It is application protocol independent.
Secure Task Execution (STE)	Secure execution of a task from a managed system. This feature of HP SMH ensures that the user requesting the task has the appropriate rights to perform the task and encrypts the request to protect data from snooping.
Security Attributes Configuration tool (secweb)	The HP-UX Security Attributes Configuration (secweb) tool is used to view and configure system-wide and per-user (local users and NIS users) values of security attributes. It also gives information about account locks. The Security Attributes Configuration tool can be launched from the HP-UX System Administration Manager (SAM) tool, or from HP SMH.
secweb	*See* Security Attributes Configuration tool .
self-signed certificate	A certificate that is its own certificate authority (CA), so that the subject and the CA are the same. *See also* certificate, certificate authority.
single sign on (SSO)	Permission granted to an authenticated user browsing to HP Systems Insight Manager (HP SIM) to browse to any of the managed systems from within HP SIM without re-authenticating to the managed system. HP SIM is the initial point of authentication and browsing to another managed system must be from within HP SIM.
software update	A task to remotely update software and firmware.
SSH	*See* Secure Shell.
SSL	*See* Secure Sockets Layer.
SSO	*See* single sign on.
status type	Systems of specified status type (Critical, Failed/Major, Degraded/Minor, Normal, and Unknown) as defined by HP SMH.
STE	*See* Secure Task Execution.
survey utility	An agent (or online service tool) that gathers and delivers hardware and operating system configuration information. This information is gathered while the server is online.
System Fault Management tool (evweb)	The System Fault Management (evweb) tool is used to view and administer WBEM indications. The evweb tool can be launched from HP SMH.
TGS	*See* Kerberos Ticket Granting Server.
ugweb	*See* Accounts for Users & Groups tool.
URI	Provides methods to access a resource on the Internet. A Uniform Resource Locator (URL) is a type of Uniform Resource Indicator (URI).
URL	A global address of resources on the World Wide Web. A Uniform Resource Locator (URL) is a type of Uniform Resource Indicator (URI).
user	A network user with a valid sign in on the HP System Management Homepage.
user accounts	Accounts used to sign in to HP System Management Homepage (HP SMH). These accounts associate a local Windows user, domain account, or an HP-UX or Linux user group with privilege levels and paging attributes inside HP SMH.
VCA	*See* HP Version Control Agent.
VCRM	*See* HP Version Control Repository Manager.
version control	Referred to as the Version Control Repository Manager installed on a Windows system for Windows and Linux Proliant or Integrity systems, and Software Distributor on HP-UX operating systems. Provides an overview of the software status for all managed ProLiant or Integrity systems and can update system software and firmware on those systems programmatically using predetermined criteria. Version control identifies systems that are running out-of-date system software, indicates if an upgrade is available, and provides reasons for upgrading. For HP-UX systems, Software Distributor can be launched from an HP Systems Insight Manager CMS against one or more installed HP-UX systems.
WBEM	*See* Web-Based Enterprise Management.

Web-Based Enterprise Management (WBEM)

Is a platform and resource independent DMTF (Distributed Management Task Force) standard that defines both a common model (for example, description) and protocol (for example, interface) for monitoring and controlling a diverse set of resources. The HP WBEM Services for HP-UX products is the HP-UX implementation of the DMTF (Distributed Management Task Force) WBEM standard.

Index

C

certificates
  trust mode, 26
  trusted management server certificates, 26
ciphers
  HP SMH, 86
CLI configuration
  HP SMH, 58
credits
  HP SMH, 56

D

documentation, 81

E

error
  log, 52
examples
  scenarios, 16

F

features, 81
file locations
  HP SMH, 84

G

getting started
  sign in, 7

H

home
  HP SMH, 25
HP SMH
  ciphers, 86

L

languages
  HP SMH, 52
logs
  error log, 52
  HP SMH, 52
  SAM log, 52
  System Management Homepage log, 52

M

manpages, 81
menu
  HP SMH, 49
MIT
  Kerberos user groups, 26

N

navigating
  HP SMH, 17

O

overview
  getting started, 7
  HP SMH, 6

P

pages
  HP SMH, 23
product overview, 6

R

reference
  troubleshooting, 79
resources, 81

S

SAM
  log, 52
scenarios
  examples, 16
  HP SMH, 16
security
  alternative name certificate, 26
  anonymous, 26
  HP SMH, 26
  IP Binding, 26
  IP Restricted sign in, 26
  Kerberos user groups, 26
  local access, 26
  local server certificate, 26
  Port 2301, 26
  trust mode, 26
  trusted management server certificates, 26
settings
  HP SMH, 26
SNMP Configuration
  HP SMH, 26

T

tasks
  HP SMH, 50
tools
  HP SMH, 51
troubleshooting
  HP SMH, 68
  reference, 79
typographic conventions, 82

U

UI Options
  HP SMH, 26
UI Properties
  HP SMH, 26
User Preferences
  HP SMH, 26

W

webapps
Integrated Agents, 55
Other Agents, 55